(19)日本国特許庁（ＪＰ）　(12) **公表特許公報（Ａ）**　(11)特許出願公表番号
特表2001－519562
（P2001－519562A）
(43)公表日　平成13年10月23日(2001.10.23)

(51)Int.Cl.'	識別記号	ＦＩ		ﾃｰﾏｺｰﾄﾞ(参考)	
Ｇ06Ｆ　12/14	320	Ｇ06Ｆ	12/14	320Ｆ	5Ｂ017
Ｇ09Ｃ　1/00	640	Ｇ09Ｃ	1/00	640Ｂ	5Ｄ044
Ｇ11Ｂ　20/10		Ｇ11Ｂ	20/10	Ｄ	5Ｊ104
	321			321Ｚ	

審査請求　未請求　予備審査請求　有　（全 71 頁）

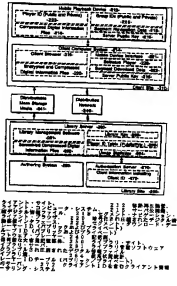
(21)出願番号　特願2000－515227(P2000－515227)
(86)（22)出願日　平成10年10月２日(1998.10.2)
(85)翻訳文提出日　平成12年４月３日(2000.4.3)
(86)国際出願番号　ＰＣＴ／ＵＳ９８／２０６５９
(87)国際公開番号　ＷＯ９９／１８５０６
(87)国際公開日　平成11年４月15日(1999.4.15)
(31)優先権主張番号　０８／９４３，５８２
(32)優先日　平成９年10月３日(1997.10.3)
(33)優先権主張国　米国（ＵＳ）

(71)出願人　オーディブル・インコーポレーテッド
アメリカ合衆国・07470・ニュージャージイ洲・ウエイン・ウイロウブルック　プルーバード・65
(72)発明者　モット，ティモシイ
アメリカ合衆国・83340・アイダホ州・ケッチャム・ビーオーボックス　6289・オールド　ミル　ロード・110
(72)発明者　ストーリイ，ガイ
アメリカ合衆国・10012・ニューヨーク州・ニューヨーク・スプリング　ストリート・151
(74)代理人　弁理士　山川　政樹

最終頁に続く

(54)【発明の名称】　デジタル情報再生装置をターゲティングする方法と装置

(57)【要約】
デジタル情報再生装置（２１２）をターゲティングする方法、装置、および製品。再生装置に装置ＩＤ（２２３）および／またはグループＩＤ（２２５）が埋め込まれる。デジタル情報ファイル（２１６）にも装置ＩＤまたはグループＩＤが埋め込まれる。デジタル情報ファイルが受信されると、再生装置の装置ＩＤまたはグループＩＤが、デジタル情報ファイルに含まれる装置ＩＤまたはグループＩＤと比較される。次いで、デジタル情報ファイルの装置ＩＤまたはグループＩＤが再生装置の装置ＩＤまたはグループＩＤと一致する場合、デジタル情報ファイルが再生される。



【特許請求の範囲】

【請求項１】　デジタル情報再生装置をターゲティングする方法であって、

再生装置に第１の装置識別子を埋め込むステップと、

デジタル情報ファイルに第２の装置識別子を埋め込むステップと、

再生装置にデジタル情報ファイルを与えるステップと、

第１の装置識別子と第２の装置識別子を比較するステップと、

第１の装置識別子が第２の装置識別子と一致する場合にデジタル情報ファイルを再生するステップと

を含むことを特徴とする方法。

【請求項２】　第１の装置識別子を埋め込むステップが、再生装置に固有の識別子を埋め込むステップを含むことを特徴とする請求項１に記載の方法。

【請求項３】　第２の装置識別子を埋め込むステップが、デジタル情報ファイルのヘッダ・ブロックに第２の装置識別子を埋め込むステップを含むことを特徴とする請求項１に記載の方法。

【請求項４】　さらに、デジタル署名アルゴリズムを実行してヘッダ・ブロックを認証するステップを含むことを特徴とする請求項３に記載の方法。

【請求項５】　さらに、

デジタル情報ファイルのあるセクションの第１のコード化値を算出するステップと、

デジタル情報ファイルに第１のコード化値を埋め込むステップと、

再生装置にデジタル情報ファイルが与えられるときに第２のコード化値を算出するステップと、

第１のコード化値が第２のコード化値と一致する場合にデジタル情報ファイルを再生するステップとを含むことを特徴とする請求項１に記載の方法。

【請求項６】　第１のコード化値を埋め込むステップが前記セクションに安全ハッシュ値を埋め込むステップを含むことを特徴とする請求項５に記載の方法。

【請求項７】　さらに、

再生装置に第１のグループ識別子を記録するステップと、

デジタル情報ファイルに第２のグループ識別子を埋め込むステップと、

第１のグループ識別子と第２のグループ識別子を比較するステップと、

第１のグループ識別子が第２のグループ識別子と一致する場合に、デジタル情報ファイルを再生するステップとを含むことを特徴とする請求項１に記載の方法。

【請求項８】　第１のグループ識別子を記録するステップが、グループ識別子をリモート電子供給源から電子的に受信するステップを含むことを特徴とする請求項７に記載の方法。

【請求項９】　第２のグループ識別子を埋め込むステップが、デジタル情報ファイルのヘッダ・ブロックに第２のグループ識別子を埋め込むステップを含むことを特徴とする請求項７に記載の方法。

【請求項１０】　さらに、デジタル署名アルゴリズムを実行してヘッダ・ブロックを認証することを特徴とする請求項９に記載の方法。

【請求項１１】　さらに、デジタル署名アルゴリズムを実行してデジタル情報ファイルを認証することを特徴とする請求項１に記載の方法。

【請求項１２】　さらに、デジタル署名アルゴリズムを実行してデジタル情報ファイルのあるセクションを認証することを特徴とする請求項１に記載の方法。

【請求項１３】　キーボード、ポインティング・デバイス、ビジュアル・ディスプレイ、およびデータ記憶装置を有し、デジタル情報再生装置をターゲティングするコンピュータ・システムで使用される、コンピュータ使用可能媒体を備えた製品であって、その媒体にはコンピュータ可読プログラム・コードが記録されており、そのプログラム・コードが、

コンピュータに、再生装置に第１の装置識別子を埋め込むませるように、コンピュータ使用可能媒体に記録されたコンピュータ可読プログラム・コードと、

コンピュータに、デジタル情報ファイルに第２の装置識別子を埋め込ませるように、コンピュータ使用可能媒体に記録されたコンピュータ可読プログラム・コードと、

コンピュータによって、再生装置にデジタル情報ファイルを与えるように、コ

ンピュータ使用可能媒体に記録されたコンピュータ可読プログラム・コードと、

コンピュータに第１の装置識別子と第２の装置識別子を比較させるように、コンピュータ使用可能媒体に記録されたコンピュータ可読プログラム・コードと、

第１の装置識別子が第２の装置識別子と一致する場合に、コンピュータにデジタル情報ファイルを再生させるように、コンピュータ使用可能媒体に記録されたコンピュータ可読プログラム・コードと

を含むことを特徴とする製品。

【請求項１４】　コンピュータに第１の装置識別子を埋め込ませるコンピュータ可読プログラム・コードが、コンピュータに再生装置に固有の識別子を埋め込ませるためにコンピュータ使用可能媒体に記録されたコンピュータ可読プログラム・コードを含むことを特徴とする請求項１３に記載の製品。

【請求項１５】　コンピュータに第２の装置識別子を埋め込ませるコンピュータ可読プログラム・コードが、コンピュータに、デジタル情報ファイルのヘッダ・ブロックに第２の装置識別子を埋め込ませるようにコンピュータ使用可能媒体に記録されたコンピュータ可読プログラム・コードを含むことを特徴とする請求項１３に記載の製品。

【請求項１６】　さらに、コンピュータに、デジタル署名アルゴリズムを実行してヘッダ・ブロックを認証させるように、コンピュータ使用可能媒体に記録されたコンピュータ可読プログラム・コードを含むことを特徴とする請求項１５に記載の製品。

【請求項１７】　さらに、

コンピュータに、デジタル情報ファイルのあるセクションの第１のコード化値を算出させるように、コンピュータ使用可能媒体に記録されたコンピュータ可読プログラム・コードと、

コンピュータに、デジタル情報ファイルに第１のコード化値を埋め込ませるように、コンピュータ使用可能媒体に記録されたコンピュータ可読プログラム・コードと、

再生装置にデジタル情報ファイルが与えられるときに、コンピュータに第２のコード化値を算出させるように、コンピュータ使用可能媒体に記録されたコンピ

ュータ可読プログラム・コードと、

第１のコード化値が第２のコード化値と一致する場合に、コンピュータにデジタル情報ファイルを再生させるように、コンピュータ使用可能媒体に記録されたコンピュータ可読プログラム・コードとを含むことを特徴とする請求項１３に記載の製品。

【請求項１８】　コンピュータに第１のコード化値を埋め込ませるコンピュータ可読プログラム・コードが、コンピュータに、前記セクションに安全ハッシュ値を埋め込ませるようにコンピュータ使用可能媒体に記録されたコンピュータ可読プログラム・コードを含むことを特徴とする請求項１７に記載の製品。

【請求項１９】　さらに、

コンピュータに、再生装置に第１のグループ識別子を埋め込ませるように、コンピュータ使用可能媒体に記録されたコンピュータ可読プログラム・コードと、

コンピュータに、デジタル情報ファイルに第２のグループ識別子を埋め込ませるように、コンピュータ使用可能媒体に記録されたコンピュータ可読プログラム・コードと、

コンピュータに、第１のグループ識別子と第２のグループ識別子を比較させるように、コンピュータ使用可能媒体に記録されたコンピュータ可読プログラム・コードと、

第１のグループ識別子が第２のグループ識別子と一致する場合に、コンピュータにデジタル情報ファイルを再生させるようにコンピュータ使用可能媒体に記録されたコンピュータ可読プログラム・コードとを含むことを特徴とする請求項１３に記載の製品。

【請求項２０】　コンピュータに第１のグループ識別子を埋め込ませるコンピュータ可読プログラム・コードが、コンピュータに、グループ識別子をリモート電子供給源から電子的に受信させるように、コンピュータ使用可能媒体に記録されたコンピュータ可読プログラム・コードを含むことを特徴とする請求項１９に記載の製品。

【請求項２１】　コンピュータに第２のグループ識別子を埋め込ませるコンピュータ可読プログラム・コードが、コンピュータに、デジタル情報ファイルの

ヘッダ・ブロックに第２のグループ識別子を埋め込ませるように、コンピュータ使用可能媒体に記録されたコンピュータ可読プログラム・コードを含むことを特徴とする請求項１９に記載の製品。

【請求項２２】　さらに、コンピュータに、デジタル署名アルゴリズムを実行してヘッダ・ブロックを認証させるように、コンピュータ使用可能媒体に記録されたコンピュータ可読プログラム・コードを含むことを特徴とする請求項２１に記載の製品。

【請求項２３】　さらに、コンピュータに、デジタル署名アルゴリズムを実行してデジタル情報ファイルを認証させるように、コンピュータ使用可能媒体に記録されたコンピュータ可読プログラム・コードを含むことを特徴とする請求項１３に記載の製品。

【請求項２４】　さらに、コンピュータに、デジタル署名アルゴリズムを実行してデジタル情報ファイルのあるセクションを認証させるように、コンピュータ使用可能媒体に記録されたコンピュータ可読プログラム・コードを含むことを特徴とする請求項１３に記載の製品。

【請求項２５】　デジタル情報再生装置をターゲティングするシステムであって、

再生装置に第１の装置識別子を埋め込む第１の再生手段を有するデジタル・コンピュータと、

デジタル情報ファイルに第２の装置識別子を埋め込むようにデジタル・コンピュータによって操作される第２の埋込み手段と、

再生装置にデジタル情報ファイルを与えるためにデジタル・コンピュータに論理的に結合された手段と、

第１の装置識別子と第２の装置識別子を比較するようにデジタル・コンピュータによって操作される比較手段と、

第１の装置識別子が第２の装置識別子と一致する場合にデジタル情報ファイルを再生するためにデジタル・コンピュータに論理的に結合された再生手段と

を備えることを特徴とするシステム。

【請求項２６】　第１の埋込み手段がさらに、再生装置に固有の識別子を埋

め込む手段を備えることを特徴とする請求項２５に記載のシステム。

【請求項２７】　第２の埋込み手段がさらに、デジタル情報ファイルのヘッダ・ブロックに第２の装置識別子を埋め込む手段を備えることを特徴とする請求項２５に記載のシステム。

【請求項２８】　さらに、デジタル署名アルゴリズムを実行してヘッダ・ブロックを認証するようにデジタル・コンピュータによって操作される認証手段を備えることを特徴とする請求項２７に記載のシステム。

【請求項２９】　さらに、

デジタル情報ファイルのあるセクションの第１のコード化値を算出するようにデジタル・コンピュータによって操作される手段と、

デジタル情報ファイルに第１のコード化値を埋め込むようにデジタル・コンピュータによって操作される手段と、

再生装置にデジタル情報ファイルが与えられるときに第２のコード化値を算出するようにデジタル・コンピュータによって操作される手段と、

第１のコード化値が第２のコード化値と一致する場合にデジタル情報ファイルを再生するようにデジタル・コンピュータによって操作される手段とを備えることを特徴とする請求項２５に記載のシステム。

【請求項３０】　第１の埋込み手段がさらに、前記セクションに安全ハッシュ値を埋め込む手段を備えることを特徴とする請求項２９に記載のシステム。

【請求項３１】　さらに、

再生装置に第１のグループ識別子を記録するようにデジタル・コンピュータによって操作される手段と、

デジタル情報ファイルに第２のグループ識別子を埋め込むようにデジタル・コンピュータによって操作される手段と、

第１のグループ識別子と第２のグループ識別子を比較するようにデジタル・コンピュータによって操作される手段と、

第１のグループ識別子が第２のグループ識別子と一致する場合にデジタル情報ファイルを再生するようにデジタル・コンピュータによって操作される手段とを備えることを特徴とする請求項２５に記載のシステム。

【請求項３２】　第１のグループ識別子を記録する手段がさらに、グループ識別子をリモート電子供給源から電子的に受信する手段を備えることを特徴とする請求項３１に記載のシステム。

【請求項３３】　第２のグループ識別子を埋め込む手段がさらに、デジタル情報ファイルのヘッダ・ブロックに第２のグループ識別子を埋め込む手段を備えることを特徴とする請求項３１に記載のシステム。

【請求項３４】　さらに、デジタル署名アルゴリズムを実行してヘッダ・ブロックを認証するようにデジタル・コンピュータによって操作される手段を備えることを特徴とする請求項３３に記載のシステム。

【請求項３５】　さらに、デジタル署名アルゴリズムを実行してデジタル情報ファイルを認証するようにデジタル・コンピュータによって操作される手段を備えることを特徴とする請求項２５に記載のシステム。

【請求項３６】　さらに、デジタル署名アルゴリズムを実行してデジタル情報ファイルのあるセクションを認証するようにデジタル・コンピュータによって操作される手段を備えることを特徴とする請求項２５に記載のシステム。

【請求項３７】　オーディオ再生装置をターゲティングするシステムであって、

オーディオ・ファイルに装置識別子を埋め込む第１の埋込み手段を有するデジタル・コンピュータと、

オーディオ・ファイルにグループ識別子を埋め込むようにデジタル・コンピュータによって操作される第２の埋込み手段と、

再生装置にオーディオ・ファイルを与えるためにデジタル・コンピュータに論理的に結合された手段と

を備えることを特徴とするシステム。

【発明の詳細な説明】

【０００１】

（発明の分野）

本発明は、全般的にはデジタル情報送信、受信、再生システムに関し、詳細には、デジタル情報再生装置をターゲティングする方法および装置に関する。

【０００２】

（発明の背景）

デジタル・データの圧縮およびコンピュータ・システムの記憶機能の拡張における最近の技術的発展と、コンピュータ・ネットワーク・インフラストラクチャの帯域幅の増大によって、大量のデジタル情報への個人的なアクセスおよびそのような情報の使用についての新たな可能性が生まれている。この種のデジタル情報の一形態は、コンピュータ・ネットワークを介してデジタル化情報として供給されるオーディオ情報である。

【０００３】

対話型デジタル情報送信、受信、再生システムの分野で、本出願人にはいくつかの特許が知られている。１９９２年７月２１日にＹｕｒｔ等に発行された米国特許第５，１３２，９９２号（Ｙｕｒｔ）は、デジタル信号処理を使用して高データ圧縮率を実現することによってビデオおよび／またはオーディオ情報を配信するシステムについて説明している。Ｙｕｒｔ特許は、ソース・マテリアル・ライブラリから得たアイテムをフォーマット済みデータとして所定のフォーマットにする変換手段を含む送信システムについて説明している。オーディオ・データは適応差分パルス符号変調（ＡＤＰＣＭ）プロセスをオーディオ・データに適用することによってオーディオ・コンプレッサによって圧縮される。記憶されたアイテムは、記憶コード化中に各アイテムに割り当てられる固有のアドレス・コードを使用することによって圧縮データ・ライブラリにおいてアクセスされる。この固有のアドレス・コードは、Ｙｕｒｔ送受信プロセス全体にわたって情報およびアイテムを要求しそれらにアクセスするために使用される。Ｙｕｒｔ送信システムは、システムがユーザ・アカウントにアクセスするための顧客識別子（ＩＤ）コードをユーザが入力するための手段を含み、ユーザがシステムの加入者であ

ることをシステムに示す。加入者に問題がない場合、Ｙｕｒｔシステムは、前述の技法を使用して、選択されたタイトルを供給する。

【０００４】

Ｙｕｒｔに記載されたオーディオ送受信システムの１つの重要な問題は、デジタル情報ライブラリのセキュリティと、デジタル情報ライブラリからユーザにダウンロードされるアイテムのセキュリティとを確保する有効な手段がないことである。Ｙｕｒｔは、ライブラリ内のアイテムに割り当てられる固有のＩＤコードと、特定のユーザに割り当てられる顧客ＩＤコードとの使用法について説明しているが、クローン・ライブラリを許可なしで作成するか、あるいはライブラリ・アイテムを許可なしでダウンロードまたはコピーするのを防止する認証プロトコルや暗号化技法については説明していない。第２に、Ｙｕｒｔおよび関連する従来技術は、移動再生装置のインタフェースを有するクライアント・コンピュータ・システムをサポートするサーバ・ベースのデジタル情報ライブラリとの間で安全なトランザクションを行う認証手段や暗号化手段については説明していない。第３に、従来技術は、確認すべきデジタル情報パッセージを選択する機構について説明していない。従来技術のシステムは、移動再生装置でどのくらいの記憶空間が使用できるかに応じてプログラムの一部のみをクライアント・コンピュータ・システムから移動再生装置にダウンロードするためのシステムについても説明していない。従来技術のシステムは、デジタル情報ライブラリから移動再生装置にダウンロードすべき複数のプログラムを指定する機能についても説明していない。従来技術のシステムは、デジタル情報ライブラリのコンテントを生成するためにオーサリング・システムで必要とされるプロセスについて詳しく説明していない。最後に、従来技術のシステムは、ライブラリ・コンテント・プロバイダが、ライブラリ・アイテムのアクセスに関する使用情報に対する問合せをリアルタイムに実行するためのアカウント・システムについても説明していない。

【０００５】

（発明の概要）

本発明は、デジタル情報再生装置をターゲティングする方法、装置、および製品を提供する。装置ＩＤまたはグループＩＤが再生装置に組み込まれる。デジタ

ル情報ファイルにも装置ＩＤまたはグループＩＤが組み込まれる。デジタル情報ファイルが受信された後、再生装置の装置ＩＤまたはグループＩＤが、デジタル情報ファイルに含まれる装置ＩＤまたはグループＩＤと比較される。次いで、デジタル情報ファイルの装置ＩＤまたはグループＩＤが再生装置の装置ＩＤまたはグループＩＤと一致する場合、このデジタル情報ファイルが再生される。

【０００６】

本発明は、添付の図面を参照して例として示され、限定的なものではない。同じ参照番号は同様の要素を示す。

【０００７】

（本発明の好ましい実施形態の詳細な説明）

本発明の好ましい実施形態は、クライアント・コンピュータ・システムおよびクライアント・コンピュータ・システムに着脱可能に接続することのできる移動デジタル情報再生システムにデジタル情報ライブラリ・プログラムを安全に転送するために認証プロトコル、ターゲティング・プロトコル、および暗号化プロトコルを使用するコンピュータ・ネットワーク・ベースのデジタル情報ライブラリ・システムである。以下の詳細な説明では、本発明を完全に理解していただくために多数の特定の詳細について述べる。しかし、当業者には、これらの特定の詳細を使用しなくても本発明を実施できることが明らかになろう。他の例では、本発明を不必要に曖昧にしないように、周知の構造、インタフェース、およびプロセスは詳しく示していない。

【０００８】

図１は、本発明の一実施形態が実現される典型的なデータ処理システムを示す。しかし、当業者には、様々なシステム・アーキテクチャの他の代替システムも使用できることが明らかになろう。図１に示すデータ処理システムは、情報を伝達するバスまたはその他の内部通信手段１０１と、情報を処理するためにバス１０１に結合されたプロセッサ１０２とを含む。システムはさらに、情報およびプロセッサ１０２によって実行される命令を記憶するためにバス１０１に結合されたランダム・アクセス・メモリ（ＲＡＭ）またはその他の揮発性記憶装置１０４（メイン・メモリと呼ばれる）を備える。メイン・メモリ１０４は、プロセッサ

１０２によって命令が実行される間に一時変数または他の中間情報を記憶するために使用することもできる。システムは、プロセッサ１０２用の静的情報および命令を記憶するためにバス１０１に結合された読取り専用メモリ（ＲＯＭ）および／または静的記憶装置１０６と、磁気ディスク・ドライブや光ディスク・ドライブなどの大容量記憶装置１０７も備える。大容量記憶装置１０７は、バス１０１に結合され、通常は、情報および命令を記憶するために磁気ディスクや光ディスクなどのコンピュータ可読大容量記憶媒体１０８と共に使用される。システムはさらに、コンピュータ・ユーザに情報を表示するためにバス１０３を介してバス１０１に結合された陰極線管（ＣＲＴ）や液晶ディスプレイ（ＬＣＤ）などの表示装置１２１に結合することができる。情報およびコマンド選択肢をプロセッサ１０２に伝達するために、英数字キーおよびその他のキーを含む英数字入力装置１２２をバス１０３を介してバス１０１に結合することもできる。追加のユーザ入力装置としては、バス１０３を介してバス１０１に結合されたマウスや、トラックボールや、スタイラスや、カーソル方向キーなどのカーソル制御装置１２３がある。これらで方向情報およびコマンド選択肢をプロセッサ１０２に伝達し表示装置１２１上のカーソル移動を制御する。任意選択でバス１０３を介してバス１０１に結合できる他の装置は、紙、フィルム、または同様な種類の媒体などの媒体上に命令、データ、またはその他の情報を印刷するために使用できるハード・コピー装置１２４である。好ましい実施形態では、通信装置１２５は、ネットワーク・コンピュータ・システムの他のノードまたは他のコンピュータ周辺装置にアクセスする際に使用できるようにバス１０３を介してバス１０１に結合される。この通信装置１２５は、イーサネット、トークン・リング、インターネット、またはワイド・エリア・ネットワークに結合するために使用されるようないくつかの市販のネットワーク化周辺装置のうちの任意の周辺装置を含むことができる。通信装置１２５は、スキャナや、端末や、専用プリンタや、オーディオ入出力装置などのリモート・コンピュータ周辺装置と通信するように設計された任意の数の市販の周辺装置を含むこともできる。通信装置１２５は、ＲＳ２３２またはその他の従来型のシリアル・ポート、従来型のパラレル・ポート、ＳＣＳＩポート、またはその他のデータ通信手段を含むこともできる。通信装置１２５は

、赤外線ＩＲＤＡプロトコルや、スペクトラム拡散や、無線ＬＡＮなどの無線データ転送装置手段を使用することができる。また、通信装置１２５は好ましい実施形態では、以下で詳しく説明するように移動再生装置２１２をクライアント・コンピュータ・システム２１４に結合するために使用される。好ましい実施形態で使用される他の１つの装置は、取り付けられたスピーカまたはヘッドフォン１３２を有するか、あるいは外部増幅器およびスピーカ、カセット・アダプタなどのオーディオ再生機器に入力するのに適したアナログ・オーディオ出力を有する音声回路１３０である。音声回路１３０は、オーディオ・ファイルを再生する技術分野でよく知られている。別法として、音声回路は、オーディオ・データを無線受信機によって受信され再生されるように予め決められている周波数上で送信する無線送信機でよい。他の無線方法も可能である。

【０００９】

図１に示すシステムの任意の構成要素またはすべての構成要素および関連するハードウェアを本発明の様々な実施形態で使用できることに留意されたい。しかし、当業者には、システムの任意の構成を特定の実装による様々な目的に使用できることが理解されよう。本発明の一実施形態では、図１に示すデータ処理システムはＩＢＭ（登録商標）互換パーソナル・コンピュータ（ＰＣ）、ＡｐｐｌｅＭａｃＩｎｔｏｓｈ（登録商標）パーソナル・コンピュータ、またはＳＵＮ（登録商標）ＳＰＡＲＣ Ｗｏｒｋｓｔａｔｉｏｎである。プロセッサ１０２は、Ｓａｎｔａ Ｃｌａｒａ、ＣａｌｉｆｏｒｎｉａのＩＮＴＥＬ（登録商標）Ｃｏｒｐｏｒａｔｉｏｎによって製造されている８０４８６またはＰＥＮＴＩＵＭ（登録商標）ブランド・マイクロプロセッサなどの８０×８６互換マイクロプロセッサのうちの１つでよい。

【００１０】

本発明を実現するソフトウェアは、メイン・メモリ１０４、大容量記憶装置１０７、またはプロセッサ１０２からアクセスできるその他の記憶媒体に記憶することができる。当業者には、本明細書で説明する方法およびプロセスを、メイン・メモリ１０４または読取り専用メモリ１０６に記憶されプロセッサ１０２によって実行されるソフトウェアとして実現できることが明らかになろう。このソフ

トウェアは、コンピュータ可読プログラム・コードを有するコンピュータ使用可能大容量記憶媒体１０８を備える製品上に存在することもでき、コンピュータ可読プログラム・コードは、コンピュータ使用可能大容量記憶媒体内に実装され、大容量記憶装置１０７によって読み取ることができ、プロセッサに本明細書の教示に従ってデジタル情報ライブラリ・トランザクションおよびプロトコルを実行させることができる。

【００１１】

デジタル情報ライブラリ・システム

図２は、本発明の好ましい実施形態で使用されるコンピュータ・ネットワーク・アーキテクチャを示す。一般に、本発明のネットワーク・アーキテクチャは、従来型の配信網インフラストラクチャ２４０を介してクライアント・サイト２１０に結合されたライブラリ・サイト２５０を含む。この従来型の配信網インフラストラクチャ２４０は、インターネット・プロバイダを介してライブラリ・サイト２５０とクライアント・サイト２１０との間に設けられる標準電話接続として実現することができ、従来型の電話網を介したインターネット上のデータ通信を可能にする。このようなインターネットの配信網としての使用法は、当業者によく知られている。ケーブル・モデム機能を有する代替実施形態では、電話網を介した通信の代わりに従来型のケーブル網を介した通信が可能である。ケーブル網は通常、標準電話網よりもずっと高速である（すなわち、ずっと大きな帯域幅を与える）。しかし、ケーブル・モデムは標準ＰＯＴＳ（単純な在来型電話サービス）モデムよりも高価である。従来型の総合サービス・デジタル網（ＩＳＤＮ）機能を有する他の代替実施形態では、配信網２４０はＩＳＤＮモデムを使用してアクセスされる。この場合も、ＩＳＤＮ網は通常、ＰＯＴＳ網よりも高速である。しかし、ＩＳＤＮ網へのアクセスは一般に、より費用がかかる。ケーブル・モデムおよびＩＳＤＮ実装は、ＰＯＴＳ実装の代替通信媒体である。

【００１２】

また、当業者には、他の形態のネットワーク化を本発明によって同様にサポートできることが明らかになろう。たとえば、赤外線リンクや無線リンクなどの無線送信手段も、本出願で説明する配信網２４０を形成することができる。インタ

ーネットの代替策として、ＡＭＥＲＩＣＡ－ＯＮ－ＬＩＮＥ（ＡＯＬ）やＣＯＭＰＵＳＥＲＶＥなど独自のネットワーク／掲示板を使用することができる。

【００１３】

ライブラリ・サイト２５０の各サーバおよびクライアント・サイト２１０のクライアント・コンピュータ・システム２１４は、上記で図１に関連して説明したようなコンピュータ・システムとして実現することができる。当業者には、前述の技法を使用して、ライブラリ・サーバ２６０、オーサリング・システム２８０、および認証サーバ２７０をリモートに配置し、しかも配信網としてネットワーク化できることが明らかになろう。また、本発明では、複数のライブラリ・サーバ、オーサリング・システム、および認証サーバを使用することができる。逆に、サーバを単一のマシンの独立の機能として実現することができる。これらの代替実施形態について、図４ないし図８に示し、以下に詳しく説明する。

【００１４】

移動再生装置２１２は、最小限の構成を有する低コストの独立式移動ユニットであり、ライブラリ・サーバ２６０およびクライアント・コンピュータ・システム２１４によってダウンロードされたデジタル情報ファイルまたはプログラムを受信して記憶し、移動再生装置２１２のユーザ用のデジタル情報ファイルまたはプログラムを再生する。移動再生装置２１２は、ダウンロードが行われている間にクライアント・コンピュータ・システム２１４に一時的に着脱可能に結合される。ダウンロード後、移動再生装置２１２をクライアント・コンピュータ・システム２１４から取り外し、独立式デジタル情報再生装置として使用することができる。「Ｉｎｔｅｒａｃｔｉｖｅ Ａｕｄｉｏ Ｔｒａｎｓｍｉｓｓｉｏｎ，Ｒｅｃｅｉｖｉｎｇ ａｎｄ Ｐｌａｙｂａｃｋ Ｓｙｓｔｅｍ」（米国特許出願第０８／４９０，５３７号）と題し、Ｍｏｎｔｃｌａｉｒ、ＮＪのＡｕｄｉｂｌｅ Ｗｏｒｄｓ Ｃｏｒｐｏｒａｔｉｏｎに譲渡されたする関連米国特許出願は、移動再生装置２１２の詳細を説明している。

【００１５】

本発明の好ましい実施形態は、その基本形態では、コンピュータ・ネットワークを介して必要に応じてデジタル情報プログラミングの選択を可能にするデジタ

ル情報ライブラリ・システムである。代替実施形態では、デジタル情報プログラミングがコンピュータ・ネットワークを介して選択されるが、大容量記憶媒体２４１を使用して供給される。この代替実施形態について以下に詳しく説明する。

【００１６】

このデジタル情報ライブラリは、デジタル情報プログラミング、書籍や毎日のニュースやエンターテインメント・フィーズなどのデジタル情報源から得た描画コンテント、会議および教育情報源、他のコンピュータ・システム、インターネットのワールド・ワイド・ウェブ（ＷＷＷ）上のホスト、ならびにカスタマイズされたオーディオまたはビジュアル画像プログラミングのインデックス付き集合である。他のデジタル情報コンテント源には、会議またはセミナーの議事録、講義またはスピーチの資料、言語レッスン、読物、コメディー、カスタマイズされたスポークン・ダイジェスト、および関連する「必須」ビジネス情報、コンピュータ・ソフトウェア、ローカル・サウンド・スタジオ・マテリアル、機械可読ファイルのテキスト・スピーチ変換、磁気テープから得られる記録済みのマテリアル、ＣＤ－ＲＯＭ、デジタル・オーディオ・テープ、またはアナログ・カセット・テープが含まれるが、これらに限らない。このデジタル情報コンテントは、図２に示すオーサリング・システム２８０への生デジタル情報コンテントとして入力される。代替実施形態では、生入力を受信し、この入力をデジタル形式に変換する生デジタル情報デジタイザ３０７が含められ、このデジタル形式をデジタル情報ファイルとして処理することができる。

【００１７】

代替実施形態では、デジタル情報は、表示画面または投影画面上でビジュアル画像を生成するために使用されるデジタル化画像またはグラフィックス・データを含む。これらの画像は、ライブラリ・サーバ２６０によって保持され、維持されるデジタル情報に含めることもできる。

【００１８】

オーサリング・システム

オーサリング・システム２８０は、デジタル情報コンテントを編集し、インデックス付けし、圧縮し、スクランブルし、セグメント化し、カタログ化してデジ

タル情報ファイル内のデジタル情報プログラムを得るために使用され、このデジタル情報プログラムは、大容量記憶媒体２４１上に記憶されるか、あるいはスクランブルされ圧縮されたデジタル情報ファイル２６２としてライブラリ・サーバ２６０上に記憶される。デジタル情報プログラムは最初、従来型の基準（たとえば、ジャンル、現代フィクション、ミステリー、アドベンチャー、ロマンス、ノンフィクション、クラシック、セルフヘルプ、サイエンス・フィクション、ウエスタンなど）に従って分類される。特定の著者または発行者に関連する範疇も与えられる。完全なタイトルと短縮タイトルの両方が与えられる。いくつかの状況では、デジタル情報コンテントを非デジタル化形式からデジタル化する必要がある。この目的のために生情報デジタイザ３０７が用意されている。オーサリング・システム２８０はまた、デジタル情報コンテントをセグメントに区画し、これらのセグメントを必要に応じて識別し、探索し、スキップすることができる。すべてのこれらの機能はオーサリング・システム２８０によって実行される。

【００１９】

図３は、好ましい実施形態のオーサリング・システム２８０を示す。オーサリング・システム２８０は、デジタル情報コンテントを様々な従来型の情報源から生デジタル化データとして受信する。このデジタル情報データは、好ましい実施形態のオーサリング・システム２８０の３つの構成要素に供給される。デジタル情報コンプレッサ３１４は、生デジタル・データを受信し、デジタル化データを圧縮する。デジタル・データを圧縮する様々な従来型の技法が存在する。これらの技法は、処理されるデジタル・データの種類に応じて最適化することができる。したがって、本発明は、いくつかの圧縮方法と、オーサリング・システム・オペレータ３０５が、デジタル情報コンプレッサ３１４に入力されるデジタル情報コンテント３１０の範疇に基づいてこれらの方法のうちの１つを選択できるようにする手段とを提供する。別法として、圧縮方法の選択は、デジタル情報コンテント３１０自体を解釈することによって自動的に実行することができる。圧縮されたデジタル情報ファイルはデジタル情報コンプレッサ３１４によってスクランブラ３１８に出力される。

【００２０】

生デジタル情報コンテント３１０はテンプレート・ヘッダ生成装置３１２にも供給される。ライブラリ・サーバ２６０によって維持される各デジタル情報ファイルは、ファイルのコンテントを識別するために使用されると共に、ファイル内のデジタル情報を処理するために使用される情報を与えるために使用される他の記述的情報を含む。各デジタル情報ファイルは、テンプレート・ヘッダ、スクランブル解除マップ、選択されたプレビュー・クリップ、およびデジタル情報プログラミング自体を含む。好ましい従来型では、テンプレート・ヘッダは、ファイル内のデジタル情報に対応するいくつかの属性を含む。たとえば、デジタル情報は、書籍または発行された他の作品のコンテントから生成されるオーディオ情報でよい。この例では、オーディオ・ファイル・テンプレート・ヘッダは、１）書籍のタイトル、巻、またはデジタル情報コンテントを得た媒体、２）デジタル情報コンテントに関連する著作権、３）コンテントの可聴タイトル、４）コンテントの目次、および５）デジタル情報を適切に再生またはレンダリングするための再生設定を含む属性を含む。目次は、章の数、プログラムの長さ、および関連コンテント・セクションを示す情報を含むがこれらに限らないコンテント・ナビゲーション情報を含む。目次は、オーサリング・システム・オペレータ３０５からの入力を用いて生成されるか、あるいはデジタル情報コンテント３１０を分析することによって自動的に生成される。スクランブル解除マップ３２２は、後述のようにスクランブラ３１８によってデジタル情報がスクランブルされた後でデジタル情報を解釈するために使用される。プレビュー・クリップ３２４は、特定のデジタル情報ファイルのコンテントの概略を消費者に示すために使用されるデジタル情報コンテントの事前に生成された短い部分を含む。好ましい実施形態では、このようなプレビューは、音声生成回路１３０によって直接再生するか、あるいは他の手段によってレンダリングすることのできる従来型のフォーマット済みファイルとして生成される。デジタル情報ファイルにはいくつかのプレビュー・クリップを関連付けることができる。好ましい実施形態では、プレビュー・クリップ３２４は圧縮されることもあるいはスクランブルされることもない。テンプレート・ヘッダ３１２は、ネットワーク２４０または大容量記憶媒体２４１に転送される際にデジタル情報ファイルを保持する。デジタル情報ファイル用の他の

記述的情報は通常、デジタル情報ファイルと共に記憶されるが、そのように記憶する必要はない。

【００２１】

再び図３を参照するとわかるように、テンプレート・ヘッダ生成装置３１２は、デジタル情報コンテント３１０の特定の部分からテンプレート・ヘッダを生成する。ヘッダ生成プロセス中にオーサリング・システム・オペレータ３０５およびデジタル情報コンプレッサ３１４からの入力を要求することができる。テンプレート・ヘッダはライブラリ・サーバ２６０に与えられる。デジタル情報ファイル・ヘッダの他の部分はスクランブラ３１８およびプレビュー生成装置３２３から与えられる。デジタル情報ファイル・ヘッダのこれらの部分は、ライブラリ・サーバ２６０によってアセンブルされ、特定のデジタル情報ファイル用のヘッダが得られる。デジタル情報ファイルの残りの部分には、圧縮されスクランブルされセグメント化されたデジタル情報コンテントが満たされる。

【００２２】

デジタル情報コンプレッサ３１４が、デジタル情報の範疇に適した選択された圧縮方法を使用して生デジタル情報を圧縮した後、スクランブラ３１８がデジタル情報をスクランブルする。デジタル情報は、許可されていない消費者がこのデジタル情報を使用するのを防止するためにスクランブルされる。好ましい実施形態では、スクランブラ３１８は従来型の暗号化方法を使用してデータを使用不能にする。スクランブルされたデジタル情報ファイルをスクランブル解除する手段となる、対応するスクランブル解除マップ３２２が生成される。スクランブリング・マップ３１６は、デジタル情報ファイルをスクランブルするためにスクランブラ３１８によって使用される。スクランブラ３１８は、デジタル情報ファイル全体、またはデジタル情報ファイルの選択された重大なサブセットを暗号化することができる。スクランブリングのレベルは、オーサリング・システム２８０、移動再生装置２１２、および／またはクライアント・コンピュータ・システム２１４上の予想されるソフトウェア・プレーヤー２２６の機能に応じて選択することができる。代替実施形態では、スクランブラ３１８の代わりに独自のデジタル情報フォーマットが使用される。

【００２３】

スクランブルされたデジタル情報コンテントは、スクランブラ３１８によってセグメント化論理３２６に出力される。セグメント化論理３２６は、デジタル情報コンテントを、移動再生装置２１２またはソフトウェア・プレーヤー２２６に効率的に記憶されかつ転送され、かつ再生中に効率的にナビゲートされるブロックに区画する。トランスポート完全性データが生成され、セグメント化されたデジタル情報に付加される。代替実施形態では、セグメント化プロセスの一部をデジタル情報コンプレッサ３１４およびスクランブラ３１８の前または後に行うことができる。テンプレート・ヘッダ生成装置３１２によって、ヘッダ生成プロセスでセグメント化情報を使用することができる。圧縮され、スクランブルされ、セグメント化されたデジタル情報ブロックは、オーサリング・システム２８０によってライブラリ・サーバ２６０に与えられる。ライブラリ・サーバ２６０は、デジタル情報コンテントの特定のアイテムに関するセグメント化されたデジタル情報ブロック、スクランブル解除マップ３２２、プレビュー・クリップ３２４、およびテンプレート・ヘッダ３１２をアセンブルしてデジタル情報プログラム・ファイルを得る。このデジタル情報プログラム・ファイルはデジタル情報プログラム・ファイル記憶領域２６２に記憶される。他の生デジタル情報コンテントは、オーサリング・システム２８０を同様に使用してデジタル情報ファイルに変換される。

【００２４】

ライブラリ・サーバ

再び図２を参照する。ライブラリ・サーバ２６０は、オーサリング・システム２８０によって作成されたデジタル情報プログラム・ファイル２６２を維持する責任を負う。また、ライブラリ・サーバ２６０は、ネットワーク２４０を介したクライアント・コンピュータ・システム２１４からデジタル情報プログラム・ファイル２６２へのアクセスを求める要求を受信し、選択されたデジタル情報ファイルの購入および供給ならびに／または選択されたプレビュー・クリップ３２４の供給を管理する。ライブラリ・サーバ２６０は、これらのライブラリ・サーバ機能と、後述の認証プロトコルに使用されるライブラリ・キー２６３とを実行す

るライブラリ管理ソフトウェア２６１を含む。ライブラリ管理ソフトウェア２６１は、デジタル情報プログラム・ファイル２６２のアクセスおよび／または購入を求めるクライアント・コンピュータ・システム２１４の要求を受信し、これに応答する処理論理を含む。ライブラリ・サーバ２６０は、このようなクライアント要求を受信した後、認証サーバ２７０を使用して、ライブラリ・サーバ２６０または認証サーバ２７０によって生成され維持されるクライアント情報２７２を用いてこの要求を認証する。クライアント情報２７２にはクライアント識別子が含まれ、クライアント識別子は、コンテントを、個々の移動再生装置２１２またはソフトウェア・プレーヤー２２６上で再生されるようにターゲティングするために使用される。クライアント情報２７２には、クライアント個人情報、ユーザ・コンテント優先順位、クライアント課金履歴、プレーヤー使用履歴、およびプレーヤー・グループ・リストを含めることができる。代替実施形態では、この代わりにクライアント情報２７２の一部をサーバ２６０に記憶することができる。ライブラリ・サーバ２６０は、以下に詳しく説明する認証プロトコルを使用して、クライアント要求を満たすことができるかどうかを判定する。承認された場合、ライブラリ・サーバ２６０は、クライアント・コンピュータ・システム２１４によって要求されたデジタル情報プログラム・ファイルまたはプレビュー・クリップにアクセスし、選択されたプレビュー・クリップを供給するか、あるいは以下に詳しく説明する認証プロトコルを使用して暗号化され、ターゲティングされたデジタル署名付きデジタル情報ファイルを構築し、暗号化され、圧縮されたデジタル情報ファイルをネットワーク２４０を介して要求側クライアント・コンピュータ・システム２１４に転送する。クライアント・システム２１４に情報を転送する供給媒体として配信可能な大容量記憶媒体２４１を使用することもできる。この場合、クライアント・コンピュータ・システム２１４は、選択されたデジタル情報ファイル（またはそのサブセット）を後で再生できるように移動再生装置２１２に独立にダウンロードすることができる。ライブラリ・サーバ２６０はまた、デジタル情報ファイル２６２のアクセス履歴に関する使用状況統計を収集し、この使用状況データを使用状況統計記憶領域２６４に記憶する。ライブラリ・サーバ２６０は、クライアント・ブラウザ２１９、ソフトウェア・プレーヤー

２２６、および移動再生装置２１２用の命令コード・セグメント（フォームウェア）も記憶する。この命令コードは、デジタル情報ファイルを転送する場合と同様にクライアント・コンピュータ・システム２１４にダウンロードすることができる。再生装置２１２およびソフトウェア・プレーヤー２２６に関するプレーヤー構成データは、ライブラリ・サーバ２６０上に記憶され、デジタル情報ファイルおよびファームウェアを転送する場合と同様にカスタマイズまたは更新することができる。構成データには、オーディオ・プロンプト、ユーザ・インタフェース・オプション、グループＩＤ情報、および情報再生パラメータが含まれるが、これらに限らない。プレーヤー構成データは、クライアント情報２７２の必要に応じてクライアント・コンピュータ・システム２１４、ソフトウェア・プレーヤー２２６、または移動再生装置２１２に転送される。

【００２５】

ライブラリ・サーバ２６０は、クライアント・コンピュータ・システム２１４で実行されるクライアント・アプリケーション・プログラムまたはクライアント・ブラウザ２１９とのインタフェースをとる。クライアント・ブラウザ２１９は、デジタル情報ファイル２６２での所望のプログラムの探索、デジタル情報ファイル２６２に関連する選択されたプレビュー・クリップの確認、選択されたプログラムの購入、命令コード・セグメントまたはプレーヤー構成データの要求、購入されたプログラムまたはその他のマテリアルの要求側クライアント・コンピュータ・システム２１４へのダウンロードを含むが、これらに限らない様々な種類のサービスをライブラリ・サーバ２６０に要求するために使用される。

【００２６】

ライブラリ・サーバ２６０は認証サーバ２７０とのインタフェースをとり、クライアント・コンピュータ・システム２１４は、本発明の好ましい実施形態の固有の認証プロトコルおよび暗号化プロトコルを使用する。これらのプロトコルの好ましい実施形態について以下の節で説明する。

【００２７】

クライアント・コンピュータ・システム

再び図２を参照するとわかるように、クライアント・コンピュータ・システム

２１４は、消費者コンピュータ・システムまたはエンド・ユーザ・コンピュータ・システム、通常は、図１に示すサンプル・システムなどのパーソナル・コンピュータを表す。消費者は、このパーソナル・コンピュータを用いて、配信網２４０を介してデジタル情報ライブラリ・サーバ２６０のデジタル情報コンテントをブラウズし、確認し、選択し、購入し、供給させることができる。クライアント・コンピュータ・システム２１４は、クライアント・ブラウザ・ソフトウェア２１９と、移動装置インタフェース２２１と、ネットワーク２４０からダウンロードされた暗号化され圧縮されたデジタル情報ファイル２２０用の記憶域と、ソフトウェア・プレーヤー２２６と、移動再生装置２１２内の記憶セグメントを決め、デジタル情報ファイル２２０のクライアント・コンピュータ・システム２１４から移動再生装置２１２へのダウンロードを助ける、デジタル情報ファイル２２０から得られるセグメント・ダウンロード・データ２２２とを備える。クライアント・コンピュータ・システム２１４は、サーバ２６０から受信されたデジタル情報およびソフトウェア・ファイルを認証するために使用されるサーバ公開鍵２１５も含む。クライアント・ブラウザ・ソフトウェア２１９は、クライアントまたは消費者が、ライブラリ・サーバ２６０のデジタル情報ライブラリ２６２にアクセスしタイトルを購入するために用いる制御論理を実現する。クライアント・ブラウザ・ソフトウェア２１９は、サーバ２６０に構成情報または命令コードを要求し、それらをダウンロードする制御論理も実現する。クライアント・ブラウザ・ソフトウェア２１９は、直接的な人間の介入なしにこれらの動作を実行するように構成することができる。移動装置インタフェース２２１は、クライアント・コンピュータ・システム２１４から移動再生装置２１２への、制御情報、命令コード、及びデジタル情報ファイルの転送を制御するために使用されるソフトウェア・インタフェースである。暗号化され圧縮されたデジタル情報ファイル２２０は、クライアント・コンピュータ・システム２１４によって、ネットワーク２４０を介してライブラリ・サーバ２６０から受信される。代替実施形態では、ネットワーク２４０ではなく配信可能な大容量記憶媒体２４１を使用してクライアント・コンピュータ・システム２１４に情報を転送する。ソフトウェア・プレーヤー２２６は、移動再生装置２１２の動作をエミュレートすると共に、クライア

ント・コンピュータ・システム２１４の音声回路１３０およびオーディオ出力装置１３２を通してデジタル情報ファイルを再生するために使用されるソフトウェア・モジュールである。ソフトウェア・プレーヤー２２６用の命令コードおよび構成情報は、移動再生装置２１２のダウンロードまたは更新を行う場合と同様にサーバ２６０からダウンロードし更新することができる。ソフトウェア・プレーヤー２２６機能は、移動再生装置２１２の機能および動作に相当する。したがって、本明細書全体にわたって使用される「プレーヤー」の語は一般に、移動再生装置２１２とソフトウェア・プレーヤー２２６の両方に当てはまる。ソフトウェア・プレーヤー２２６には固有のプレーヤーＩＤが割り当てられ、かつ移動再生装置２１２に割り当てられるＩＤと同様に機能するグループＩＤを割り当てることができる。

【００２８】

移動再生装置

移動再生装置２１２は、デジタル情報ファイルを、オーディオ出力手段を通して再生される音声、または表示装置上に表示される表示可能な画像に変換する。好ましい実施形態では、移動再生装置２１２は、最小限の機能を有する低コストの装置であり、主としてオーディオ・ファイルの再生またはビジュアル画像またはテキストの表示装置上への表示専用に使用される。移動再生装置２１２は、軽量で低コストで容易に移動可能な特徴を保持するように最小限の構成を有する。したがって、好ましい実施形態では、ポータブル・パーソナル・コンピュータやラップトップ・コンピュータを移動再生装置２１２として使用することはない。というのは、このような汎用コンピューティング装置は通常、好ましい移動再生装置２１２の軽量制約および低コスト制約を満たさないからである。このような汎用コンピューティング装置は通常、不要な機能と複雑なインタフェースを有し、専用移動再生装置２１２と比べてコストおよび性能面の欠点を有することがある。好ましい実施形態では、移動再生装置２１２は、プロセッサ、メモリ、およびクライアント・コンピュータ・システム２１４とのインタフェースを含み、このインタフェースを介して圧縮デジタル情報ファイル２１６が受信される。以下に詳しく説明するように、移動再生装置２１２は、クライアント・コンピュータ

・システム２１４を介してサーバ２６０から受信されたデジタル情報およびソフトウェア・ファイルを認証するために使用されるプレーヤーＩＤ２２３、グループＩＤ２２５、およびサーバ公開鍵２１５も含む。ユーザは、装置上に設けられたボタンおよびノブを使用して移動再生装置２１２を制御する。これらの制御装置は、デジタル情報ファイル２１６をナビゲートするか、構成データおよび再生パラメータを調整するか、あるいは再生装置２１２に記憶されているファームウェアの指示に応じて他の機能を実行するために使用される。クライアント・コンピュータ・システム２１４あるいは他の電子装置は、プレーヤーに結合されると、これらの制御装置からのユーザ入力を要求することができる。代替実施形態では、有線接続または無線接続を介してプレーヤーに結合されたリモート制御ユニット上に１組の追加のユーザ制御装置が設けられる。ヘッドフォン・ジャックを介すか、あるいはボード・スピーカまたは無線送信機上で、スピーカまたはヘッドフォンを有する独立の無線受信機にデジタル情報出力を与えることができる。オーディオ・レベルはボリューム・ノブを用いて調整することができる。無線送信機は、送信周波数またはその他の送信パラメータを調整する調整ノブを含むことができる。ビジュアル情報出力は、ＬＣＤディスプレイまたはＬＥＤディスプレイを介して与えられるか、あるいは標準ビジュアル表示装置への出力を介して与えられる。移動再生装置２１２は、限られた量の非揮発性メモリ、ＲＡＭ、およびＲＯＭを含む。デジタル情報コンテント、構成データ、および命令コードは移動再生装置２１２のメモリ空間に記憶される。構成データには、パブリックＩＤおよびプライベートＩＤ、コンテント再生パラメータ、およびユーザ・インタフェース・パラメータが含まれるが、これらに限らない。非揮発性メモリを使用することによって、デジタル情報コンテント、構成データ、およびファームウェアの一部をダウンロードを介して更新することができる。デジタル情報コンテントとファームウェア（オペレーティング・ソフトウェア）は共に、このメモリ装置に記憶される。ファームウェアおよび構成情報の一部は永久的に読取り専用メモリ（ＲＯＭ）に記憶される。移動再生装置２１２のメモリのコンテントを追跡するために内部メモリ割付け方法が使用される。この割付け方法は、セグメント・ナビゲーション・データ２１８と共に、移動再生装置２１２メモリに存在する

所望のデジタル情報、プログラム、構成データ、またはヘッダ・データを見つける手段も実現する。移動再生装置２１２はクライアント・コンピュータ・システム２１４とのインタフェースを含み、このインタフェースを介して、圧縮デジタル情報ファイル２１６、ソフトウェアの更新、および構成の変更をクライアント・コンピュータ・システム２１４から受信する。

【００２９】

デジタル情報コンテント、ソフトウェアの更新、または構成情報の、ライブラリ・サーバからクライアント・コンピュータ・システムへのダウンロード

クライアント・コンピュータ・システム２１４のクライアント・ブラウザ・ソフトウェア２１９は、ライブラリ・サーバ２６０のライブラリ管理ソフトウェア２６１、および移動再生装置２１２に存在するファームウェアと協働し、消費者が配信網２４０を介してデジタル情報ライブラリ・サーバ２６０のデジタル情報コンテントをブラウズし、確認し、選択し、選択したデジタル情報コンテントを購入し、供給させることができる手段を実現する。デジタル情報コンテントは通常、購入時にクライアント・コンピュータ・システム２１４にダウンロードされるが、１）購入後のある時点で、あるいは２）最初の購入後の複数の時点で、デジタル情報コンテントをダウンロードすることが可能である。クライアント・ブラウザ２１９は、ユーザの介入なしにクライアント・コンピュータ・システム２１４にコンテントをダウンロードするように構成することができる。また、クライアント・コンピュータ・システム２１４ソフトウェア自体の一部または移動再生装置２１２常駐ソフトウェア／ファームウェアの一部をライブラリ・サーバ２６０からダウンロードまたは更新することができる。移動再生装置２１２に常駐するソフトウェア／ファームウェアはクライアント・コンピュータ・システム２１４を介してダウンロードされる。ライブラリ・サーバ２６０が、クライアント・コンピュータ・システム２１４ソフトウェアまたは移動再生装置２１２のソフトウェア／ファームウェアの更新済みコピーまたはより新しいコピーを有する場合、このライブラリ・サーバ・コピーがダウンロードされ、対応するクライアント・コンピュータ・システム２１４のソフトウェアまたは移動再生装置ソフトウェア２１２の古いバージョンに取って代わる。ソフトウェアは、デジタル情報フ

ァイルのスクランブリングおよび供給の場合と同様に暗号化され、スクランブルされ、デジタルに署名される。再生装置２１２用のＩＤリスト、オーディオ・プロンプト、およびその他の構成データに対する変更は、ライブラリ・サーバ２６０からソフトウェアの更新をダウンロードする場合と同様にダウンロードすることができる。

【００３０】

好ましい実施形態は、認証プロセスを使用してサーバ２６０からクライアント・システム２１４および再生装置２１２への情報の転送を保護する。第１に、ポイント・ツー・ポイント認証プロトコルが実行され、そのため、ライブラリ・サーバ２６０は、要求側クライアント・コンピュータ・システムが許可されたクライアントであることを検証しなければならず、クライアント・コンピュータ・システム２１４は、ライブラリ・サーバ２６０が許可されたプロバイダであることを検証しなければならない。第２に、ターゲティング・プロトコルが実行され、そのため、ライブラリ・サーバ２６０は、選択されたダウンロード・データをライブラリ・サーバ２６０から受信することを許可された移動再生装置２１２に１組の識別子（すなわち、プレーヤーＩＤ）を使用する。移動再生装置識別子は、クライアント・コンピュータ・システム２１４から与えられるか、あるいはライブラリ・サーバ２６０上に記憶されているユーザ・プロファイルから参照される。ターゲティング・プロセスで、ライブラリ・サーバ２６０は、移動装置２１２によってこのような識別子を用いないかぎり読み取ることもあるいは再生することもできないデータをフォーマットしダウンロードする。第３に、ダウンロードされたデータが許可されたライブラリ・サーバから発振されたデータであることを検証すると共に、ダウンロードされたデータの完全性を検証するために、移動再生装置２１２によって使用されるライブラリ・サーバ・デジタル署名が、ダウンロードされたデータに付加される。本発明のこの３つの認証プロセスについて以下に詳しく説明する。

【００３１】

ポイント・ツー・ポイント認証プロトコル

ライブラリ・サーバ２６０、クライアント・コンピュータ・システム２１４、

および移動再生装置２１２はそれぞれ、他のシステムの真正さを検証するために使用される固有の検証シーケンスを有する。ライブラリ・サーバ２６０とクライアント・システム２１４との間の通信で、２つのシステムは交互に、（１）他のシステムの検証を要求し、（２）検証要求に対する認証応答を与えるように動作する。移動装置２１２とクライアント・コンピュータ・システム２１４との間の通信では、同様な認証プロトコルが使用されると共に、クライアント・システム２１４を介した移動装置２１２とライブラリ・サーバ２６０との間のリアルタイム通信が使用される。この検証シーケンスは、事前に決められている１組のビット・ストリームまたはデータ構造を含み、これらのビット・ストリームまたはデータ構造は、ポイント・ツー・ポイント送信で認証されている受信側システム（すなわち、受信側）に要求側システム（すなわち、検証を要求しているシステム）から送信される。受信側システムは、特定の応答ビット・ストリームまたはデータ構造を要求側システムに送信することによって、予め決められている方法で検証シーケンスに応答しなければならない。応答側からの適切な応答データが要求側システムによって受信された場合、検証中のシステムは、許可されたシステムとみられる。逆に、予め決められているタイムアウト期間が満了する前に、要求側システムによって適切な応答データが受信されなかった場合、検証中のシステムは許可されていないとみられる。２つのシステムは、別々の検証サイクルで要求側および応答側として働くことによって通信を開始する。これらのポイント・ツー・ポイント認証サイクルが完了した後、両方のシステムが互いを許可されたシステムであると判断した場合にのみ、さらなるクライアント／サーバ処理が継続する。

【００３２】

代替実施形態では、ライブラリ・サーバ２６０、クライアント・コンピュータ・システム２１４、および移動再生装置２１２の間の通信サブセットでポイント・ツー・ポイント認証が使用される。他の実施形態では、ポイント・ツー・ポイント認証は使用されず、システム・セキュリティはターゲティングおよび／またはデジタル署名認証の使用に依存する。

【００３３】

ターゲティング・プロトコル

本発明のターゲティング・プロトコルは、デジタル情報コンテントの再生、プレーヤー構成データの調整、および指定されたプレーヤー２１２／２２６または指定された１組の移動再生装置２１２へのプレーヤー命令コードのダウンロードを制限する手段および方法である。各プレーヤー２１２／２２６は固有のプレーヤＩＤ２２３を含む。プレーヤＩＤ２２３はパブリック・プレーヤＩＤおよびプライベート・プレーヤＩＤを含む。パブリック・プレーヤＩＤは固有の識別子であり、プレーヤーを識別するための通し番号として働く。プライベート・プレーヤＩＤは、個々の移動再生装置２１２用のデータをターゲティングするために使用される。インストール中を除いて、プライベート・プレーヤＩＤが通信リンクやネットワーク・パスを介して送信されることはない。好ましい実施形態では、各プライベート・プレーヤＩＤは十分に離散すべきであるが、固有のＩＤである必要はない。

【００３４】

移動再生装置２１２は、グループＩＤを使用して論理的にグループ分けすることができる。デジタル情報コンテント、ソフトウェア、または構成データは、グループＩＤによって決まる１群の移動再生装置２１２をターゲティングすることができる。各プレーヤー２１２／２２６は、特定のプレーヤー２１２／２２６がメンバーである１つまたは複数のグループＩＤ２２５を記憶するためのメモリ空間を含む。各グループＩＤはパブリック部およびプライベート部を含み、これらの部分はそれぞれ、パブリック・プレーヤＩＤおよびプライベート・プレーヤＩＤに相当する。各グループは、他のプレーヤＩＤやグループＩＤと共用されない固有の値のパブリックＩＤによって識別される。デジタル情報コンテント、ソフトウェア、または構成データは、特定のプレーヤＩＤのターゲティングの場合と同様に特定のグループＩＤをターゲティングすることができる。同じグループ内の移動再生装置２１２は同じグループＩＤを共用する。特定のグループＩＤは、すべての移動再生装置２１２がメンバーであるグローバル・グループとして事前に決められる。移動再生装置２１２は、複数のグループのメンバーでよい。特定のプレーヤー２１２／２２６に維持されている１組のグループＩＤに新

しいグループＩＤを付加することによって、特定のプレーヤー２１２／２２６が新しいグループに追加される。この新しいグループＩＤは、サーバ２６０がパブリック・グループＩＤおよびグループ鍵をクライアント・コンピュータ・システム２１４を介してプレーヤー２１２／２２６に与えた後で付加される。プレーヤー２１２／２２６は、グループ鍵と移動再生装置２１２のプライベート・プレーヤーＩＤとの組合せからプライベート・グループＩＤを生成する。プライベート・プレーヤーＩＤの場合と同様に、インストール中を除いて、プライベート・グループＩＤが通信リンクやネットワーク・パスを介して送信されることはない。代替実施形態では、プレーヤーは、グループ・プライベートＩＤを直接、あるいはグループ鍵をプレーヤー・パブリックＩＤまたは他の既知の数値と組み合わせることによって受信する。他の代替実施形態では、プライベート・グループＩＤは、ターゲティング・プロセスでは使用されず、プレーヤーには転送されない。グループ割当てプロセスは、クライアント・システム２１４を介してサーバ２６０とプレーヤーとの間でリアルタイム通信を使用することに制限するか、あるいはグループ割当てがクライアント・システム２１４にダウンロードされた後のある時点で行うことができる。本発明で決められるプレーヤーＩＤおよびグループＩＤについて説明したが、次にターゲティング・プロトコルにおけるこれらのＩＤの使用法について説明する。

【００３５】

ライブラリ・サーバ２６０は、図２に示すプレーヤーＩＤテーブル２６６を含む。プレーヤーＩＤテーブル２６６は、プライベートＩＤおよびパブリックＩＤ用の記憶領域を含む。プライベートＩＤは、新しい移動再生装置がシステムにインストールされたときか、あるいは新しいグループが確立されたときにプレーヤー・テーブル２６６にプリロードされる。他の実施形態では、ＩＤテーブル２６６は数学的関数であり、グループ・パブリックＩＤまたはプレーヤー・パブリックＩＤを変換する。クライアント・コンピュータ・システム２１４が特定のプレーヤー２１２／２２６または１組の移動再生装置２１２を特定の指定されたデジタル情報、ソフトウェア・コンテント、または選択された構成データにターゲティングする必要があるときに、クライアント・コンピュータ・システム２１４に

よってパブリック・プレーヤーＩＤおよびパブリック・グループＩＤがサーバ２６０に送信される。デジタル情報の選択は、ライブラリ・サーバ２６０上に記憶されているファイル２６２から行われる。ソフトウェアまたは構成データの選択は、サーバ２６０上に記憶されているファイル、またはサーバ２６０による要求に応じて生成されるデータから行われる。ソフトウェア・コンテントおよび構成データは、デジタル情報コンテントに対するオーサリング・プロセスと同様に作成されスクランブルされる。クライアント・コンピュータ・システム２１４によって１組のターゲティングされたパブリックＩＤとサーバ２６０から転送すべき関連データとが関連付けされた後、ライブラリ・サーバ２６０は、選択されたファイルのターゲティングされたヘッダを作成する。ライブラリ管理ソフトウェア２６１は、パブリックＩＤープライベートＩＤテーブル２６６を参照し、対応するターゲティングされたプライベートＩＤを見つける。ターゲティングされたヘッダは、選択されたファイルから得られるスクランブル解除マップ３２２と、ターゲティングされた移動再生装置２１２に対応するプライベート・プレーヤーＩＤとの組合せを含む。したがって、ターゲティングされた移動再生装置２１２の秘密ＩＤを使用してスクランブル解除マップ３２２が暗号化される。ターゲティングされたこのヘッダは、ネットワーク・トランスポート・レディ・データ・ブロック内の選択されたファイルの対応するデジタル情報またはソフトウェア・コンテントとリンクされる。以下にデータ署名プロトコルに関連して説明するようにこのデータ・ブロックにデジタル署名が適用される。このデータ・ブロックにトランスポート完全性データ（チェックサムまたは循環冗長検査の使用など）が適用され、データ・ブロックはネットワーク２４０を介してクライアント・コンピュータ・システム２１４に送信される。対応するスクランブル解除ブロック３２２をデータ・ブロックのヘッダで使用しないかぎりデータ・ブロックをスクランブル解除することはできず、かつスクランブル解除ブロック３２２が、ターゲティングされた移動再生装置２１２しか知らないプライベートＩＤと組み合わされている（すなわち、暗号化されている）ので、このデータ・ブロックをスクランブル解除し読み取ることのできるのは、ターゲティングされた移動再生装置２１２だけである。したがって、選択されたデジタル情報、ソフトウェア・コンテ

ント、および構成データは、特定の１組の移動再生装置２１２にターゲティングされる。

【００３６】

小さな移動再生装置２１２群の場合、デジタル情報ファイルのターゲティングされた各ヘッダは複数のスクランブル解除マップを含むことができ、各スクランブル解除マップは異なるプレーヤー２１２／２２６に関連付けられる。このように、複数の移動再生装置２１２は、クライアント・コンピュータ・システム２１４上に記憶されている単一のファイル２２０を読み取ることができる。

【００３７】

当業者は、代替ターゲティング方法が存在することに留意されたい。代替実施形態では、ライブラリ・サーバ２６０は、ターゲティングされた受信側のプライベート・プレーヤー２１２／２２６識別子またはターゲティングされたグループのプライベート・グループ識別子を使用してスクランブル・マップ３１６を生成する。スクランブル解除マップ３２２は、受信側プレーヤーまたは受信側グループによってすでに知られているのでファイルと共に記憶されることはない。この方法では、単一のプレーヤー２１２／２２６またはグループにコンテントがターゲティングされ、コンテントの許可されない再生を防止する場合と同一の結果が達成される。

【００３８】

他の代替実施形態では、ライブラリ・サーバ２６０はデジタル情報コンテントをスクランブルすることも、あるいは既知の鍵を使用してデジタル情報コンテントをスクランブルすることもない。この実施形態では、スクランブル解除マップ３２２は不要であり、ファイルと共に記憶されることはない。ターゲティング識別のためにパブリック・プレーヤー２１２識別子またはプライベート・プレーヤー２２６識別子をヘッダに記憶することができる。プレーヤー２１２／２２６は、ライブラリ・サーバ２６０からデータを受信した後、プレーヤー２１２／２２６識別子またはグループ識別子がヘッダに含まれているかどうかを検査する。この方法では、未修正移動再生装置２１２が仮定され、コンテントの許可されない再生を防止する場合と同じ結果が達成される。

【００３９】

他の代替実施形態では、ユーザがライブラリ・サーバ２６０に登録しユーザのクライアントＩＤを得るときに、ターゲティングされた移動再生装置２１２のプレーヤーＩＤがクライアント・コンピュータ・システム２１４によってライブラリ・サーバ２６０に送信される。この代替実施形態では、このプレーヤーＩＤはユーザ・プロファイル内のライブラリ・サーバ２６０上に記憶される。この実施形態では、ライブラリ・サーバ２６０は、ターゲティングされた移動再生装置２１２のプレーヤーＩＤを管理する。

【００４０】

デジタル署名プロトコル

本発明で使用される第３の認証プロトコルはデジタル署名プロトコルである。ライブラリ・サーバ２６０によって生成されクライアント・コンピュータ・システム２１４にダウンロードされる選択されたデータ・ブロックに対して、ライブラリ・サーバ２６０はそのプライベート・ライブラリ鍵２６３を使用してこのデータ・ブロックにデジタル署名を適用する。デジタル署名は既知のビット文字列またはデータ・パターンを含み、このビット文字列またはデータ・パターンは、ライブラリ・サーバ２６０からクライアント・コンピュータ・システム２１４にダウンロードされるデータ・ブロック内のデータと組み合わされる。ライブラリ・サーバ２６０は、すべてのデータ・ブロックまたはデータ・ブロックの選択されたサブセット上でこの動作を実行することができる。データ・ブロックがクライアント・コンピュータ・システム２１４を介してプレーヤー２１２／２２６にダウンロードされた後、プレーヤー２１２／２２６は、プレーヤー２１２／２２６に知られている公開サーバ鍵を使用して、ライブラリ・サーバ２６０によって適用されるデジタル署名を検索することができる。それによって、プレーヤー２１２／２２６は、データ・ブロックが許可されたライブラリ・サーバ２６０から発信されたことを検証すると共に、データ・ブロックの完全性を検証することもできる。公開サーバ鍵はクライアント・コンピュータ・システムにも知られており、クライアント・コンピュータ・システム２１４は同一の動作を実行し、データ・ブロックが許可されたライブラリ・サーバ２６０から発信されたことを検証

する。この実施形態では、ライブラリ・サーバ２６０はコンテント上で署名を実行する。当業者には、オーサリング・システム２８０によってデジタル情報にも署名を実行できることが認識されよう。署名は、オーサリング・システム２８０およびライブラリ・サーバ２６０によって共用される多重ステップ・プロセスで実行することもできる。

【００４１】

代替実施形態では、信頼できるクライアント・コンピュータ・システム２１４によって、ダウンロードされたマテリアルにデジタル署名が適用される。他の代替実施形態では、デジタル署名は、ダウンロードされたマテリアルには適用されず、システム・セキュリティはターゲティングおよび／またはポイント・ツー・ポイント認証の使用に依存する。

【００４２】

クライアント・コンピュータ・システムから移動再生装置への、デジタル情報コンテント、ソフトウェアの更新、または構成情報のダウンロード

第１のステップでは、クライアント・コンピュータ・システム２１４および移動装置は、前述のポイント・ツー・ポイント認証プロトコルを使用して、許可された移動再生装置２１２が許可されたクライアント・コンピュータ・システム２１４と通信していることを検証する。そうである場合、移動再生装置２１２は、そのメモリ・マップを移動装置インタフェース２２１を介してクライアント・コンピュータ・システム２１４に送信する。クライアント・コンピュータ・システム２１４に存在する利用可能なデジタル情報ファイル２２０およびプレーヤー構成プロファイルを決める目次が、クライアント・コンピュータ・システム２１４のユーザ用の移動再生装置２１２メモリ・マップと共に表示される。ユーザは、指定された移動再生装置２１２メモリの、移動再生装置２１２メモリ・マップによって決められる部分またはセグメントをクライアント・コンピュータ・システム２１４のどのファイル２２０で置き換えるべきかを選択する。別法として、この選択プロセスを自動的に実行するようにクライアント・ブラウザ２１９を構成することができる。いずれの場合も、ユーザが再生装置２１２の利用可能なメモリよりも大きなデジタル情報コンテントを選択することは防止される。また、再

生装置２１２用の制御ソフトウェアおよび／または構成データをクライアント・コンピュータ２１４によって自動的に更新することができる。その後、指定されたデジタル情報ファイル２２０、関連するヘッダ、命令コード、または構成データは、移動再生装置２１２メモリにダウンロードされる。移動再生装置２１２は、チェックサムを使用してこのダウンロードの完全性を検証する。移動再生装置２１２は、サーバ公開鍵２１５、ヘッダ、およびデジタル署名を使用して、前述のようにダウンロードを認証する。ヘッダ・スクランブル解除マップは、ダウンロードされたデータをスクランブル解除するために、ターゲティングされた移動再生装置２１２によって使用される。他の実施形態では、移動再生装置２１２は、署名を認証する前に、ダウンロードされたデータをスクランブル解除し、かつ／または圧縮解除しておくことができる。デジタル情報コンテントの各セグメントは、前述の技法を使用して独立に認証し、かつ妥当性を検査することができる。移動再生装置２１２上のデジタル情報プロンプトは、ダウンロードされたデータのヘッダに存在する目次によって指定される、ダウンロードされたデジタル情報コンテントの所望の部分にユーザを導く。ユーザは、プレビュー・オプションを選択することによってデジタル情報コンテントの選択された部分を確認することができる。プレビュー・オプションは、選択されたデジタル情報プログラムの所定の部分を再生する。特定のデジタル情報プログラムが選択された後、移動再生装置２１２がデジタル情報コンテントを、オーディオ出力手段を通して再生される音声、または表示装置上に表示される表示可能な画像に変換した後で、選択されたデジタル情報プログラムがユーザに対して再生される。

【００４３】

クライアント・コンピュータ・システム２１４のソフトウェア・プレーヤー２２６は、移動再生装置２１２にダウンロードされたデジタル情報コンテントとほぼ同じ形式でデジタル情報コンテントを受信することもできる。しかし、ソフトウェア・プレーヤー２２６用のデジタル情報コンテントをソフトウェア・プレーヤー２２６にダウンロードする必要はない。ソフトウェア・プレーヤー２２６は、クライアント・コンピュータ・システム２１４とメモリおよび／またはディスク記憶空間を共用するので、デジタル情報コンテントに直接アクセスすることが

できる。したがって、ダウンロードやメモリ・マップに関する問題は生じない。ソフトウェア・プレーヤー２２６は、移動再生装置２１２の場合と同様に、デジタル署名検証、チェックサムの検証、ターゲティングされた情報の受信を行う。代替実施形態では、ソフトウェア・プレーヤー２２６は、デジタル情報コンテント、構成情報、および動的にダウンロードされたソフトウェアを受信する際に移動再生装置２１２の通信プロトコルと同様な通信プロトコルを使用する。

【００４４】

図４は、本発明の代替実施形態を示す。図４に示すように、オーサリング・システム２８０は複数のライブラリ・サーバ２６０をサポートすることができる。各ライブラリ・サーバは特定の種類のデジタル情報コンテントをサポートするように構成することができる。上記で説明したのと同様に、クライアント・コンピュータ・システム２１４は、前述の認証プロセスを実行した後で、ネットワーク２４０にアクセスし任意のライブラリ・サーバ２６０からデジタル情報コンテントを得る。この目的のために許可サーバ２７０が設けられる。図４に示す構成は、より分散型のアーキテクチャを実現し、それによって負荷をいくつかのサーバ・プラットフォームに分散する。多数のクライアント・コンピュータ・システム２１４を有するサイトは、ネットワーク２４０上の要求を低減するためにサイト自体のライブラリ・サーバ２６０を有することができる。このアーキテクチャは、クライアント・コンピュータ・システム２１４の数が増加し、ライブラリ・サーバ２６０から与えられるコンテントが増大するときにうまくスケーリングすることができる。

【００４５】

図５は本発明の他の実施形態を示す。ただし、単一のライブラリ・サーバ・プラットフォーム４６１上で並行して実行される複数の別々のプロセスまたはタスク４６０としてライブラリ・サーバ４６１が実現されている。各ライブラリ・サーバ・プロセス４６０は、デジタル情報コンテントの対応する部分へのアクセスを求める要求を処理する。このコンテントは、前述のようにオーサリング・システム２８０を使用して作成される。許可サーバ２７０は、クライアント・コンピュータ・システム２１４とライブラリ・サーバ・プロセス４６０との間のリンク

の妥当性を検査するために使用される。図５に示す構成は、単一のサーバの都合が維持され、同時に複数のライブラリのスケーラビリティもサポートされるという点で有利である。

【００４６】

この概念は、オーサリング・サーバ２８０および許可サーバ２７０のそれぞれに使用することもできる。図６に示すように、オーサリング・システム２８０および許可サーバ２７０は、単一のプラットフォーム６８５上でオーサリング・プロセス６８０および許可プロセス６７０として実現される。これらのプロセスは、上記と同じ機能を実行する。ただし、この実装では、単一のサーバの都合が図られ、オーサリング・タスクおよび許可タスクに関する複数のプロセスのスケーラビリティが実現される。

【００４７】

図７は、クライアント・コンピュータ・システム２１４がローカル・ライブラリ７１０を含む他の代替実施形態を示す。ローカル・ライブラリ７１０は、ローカル記憶領域ライブラリ・アクセス制御機能を実現し、この機能は、ライブラリ・サーバ２６０から保存デジタル情報のサブセットへのアクセスを可能にする。前述のように、クライアント・コンピュータ・システム２１４のユーザは、ユーザがアクセスする必要のあるライブラリ・サーバ２６０内のデジタル情報のタイトルまたはアイテムを識別する。好ましい実施形態では、選択されたこのコンテントは、（図２に示すように）クライアント記憶領域２２０に転送され、それに続いて移動再生装置２１２にダウンロードされる。図７に示す実施形態は、クライアント記憶領域２２０を拡張し、ローカル・ライブラリ７１０を作成する。ローカル・ライブラリ７１０は、選択されたコンテントを記憶するために使用され、ローカルに記憶されたコンテントを探索し、ソートし、分類し、抽象化するためにも使用される。ローカル・ライブラリ７１０は、クライアント・コンピュータ・システム２１４が完全なライブラリの小さなサブセットを維持することを可能にし、ユーザが選択した様々な構成のコンテントのカスタム集合を作成するためにこのサブセットを使用することができる。クライアント・システム２１４は、他のクライアント・システム２１４上のローカル・ライブラリ７１０のコンテ

ントにアクセスすることができる。関連する代替実施形態では、ライブラリ・サーバ・プロセス４６０は、選択されたクライアント・システム２１４上に存在することもできる。この実施形態によって、クライアント・システム２１４は、コンテントをブラウズし購入することができる。このコンテントは、スクランブルされ、ターゲティングされ、ローカルに配置されたクライアント・システム２１４上で実行されるライブラリ・サーバ・プロセス４６０から供給される。ライブラリをローカルに維持することによって、ネットワーク・アクセスおよび転送オーバヘッドの一部がなくなる。

【００４８】

図８は、本発明の他の代替実施形態を示す。この場合、クライアント・コンピュータ・システム２１４がなくなり、移動再生装置２１２がネットワーク・インタフェース８１０を介してネットワーク２４０に直接接続される。好ましい実施形態では、移動再生装置２１２は、主として、オーディオ・ファイルの再生専用あるいは表示装置上でのビジュアル画像またはテキストの表示専用の、最小限の機能を有する装置である。移動再生装置２１２は、軽量で低コストで容易に移動できる特徴を保持するように最小限の構成を有する。したがって、好ましい実施形態は、ポータブル・パーソナル・コンピュータまたはラップトップ・コンピュータの使用を含まない。というのは、このような装置は従来、好ましい移動再生装置２１２の軽量制約および低コスト制約に従わないからである。しかし、最小限の移動再生装置２１２は、従来型のハードウェア・コネクタ、ハードウェア・バッファおよびコントローラ、ならびに特定の従来型のネットワーク・プロトコルに対するファームウェア・サポートを備えるネットワーク・インタフェース８１０を追加するように強化することができる。たとえば、移動再生装置２１２は電話ジャックを含む一体型モデムで拡張することができる。この電話ジャックを用いて、再生装置を電話網に接続することができる。当業者には、移動再生装置２１２など低コストで軽量の装置でネットワーク・インタフェース８１０を実現できることが明らかであろう。図８に示す代替実施形態では、クライアント・システム・ブラウザ２１９を使用できないので、移動再生装置２１２ファームウェアまたはその他の非揮発性メモリに簡略化されたユーザ・インタフェースを設け

ることができ、ユーザは、このユーザ・インタフェースを用いて、ライブラリ・サーバ２６０からダウンロードし再生すべきデジタル情報アイテムを選択することができる。前述のように、ユーザがライブラリ・サーバ２６０コンテントにアクセスする前に移動再生装置２１２とライブラリ・サーバ２６０との間のリンクの妥当性を検査する認証プロセスも実行しなければならない。別法として、クライアント・ブラウザ２１９をサポートし、それによって、ライブラリ・サーバ２６０から任意の移動再生装置２１２に直接ダウンロードし再生すべきデジタル情報アイテムを選択できるようにするために、ネットワーク２４０に結合されたクライアント・システム８１４を設けることができる。クライアント・システム８１４は、デジタル情報、ソフトウェア、および構成データを、記憶空間２２０またはローカル・ライブラリ７１０と同様な形式でローカルに記憶することをサポートすることができる。また、ネットワーク２４０を介してライブラリ・サーバ２６０ではなくクライアント・システム８１４と通信する、ネットワーク・インタフェース８１０のより簡略化された実装を設計することができる。

【００４９】

本発明の他の代替実施形態では、前述のようにクライアント・コンピュータ・システム２１４およびライブラリ・サーバ２６０を使用して、デジタル情報プログラミングが選択される。しかし、選択されたプログラミングは大容量記憶媒体２４１上で供給される。大容量記憶媒体２４１は、ＣＤ－ＲＯＭ、ＰＣＭＣＩＡカード、ＤＶＤ、フロッピィ・ディスク、着脱可能ハード・ドライブ、デジタル磁気テープ、光カード、フラッシュ・メモリ、あるいはその他の光メモリ装置、磁気メモリ装置、電子メモリ装置、または半導体メモリ装置を含む様々な従来型の大容量記憶技法のうちの任意の技法を表わす。ユーザがクライアント・コンピュータ・システム２１４を選択すると、選択されたプログラミングが、前述のようにターゲティングされスクランブルされ、選択された大容量記憶媒体２４１に転送され、郵送されるか、あるいは手渡しされるか、あるいはユーザによって取り出せるように保持される。ユーザが、選択された大容量記憶媒体２４１を物理的に所有した後、選択されたプログラミングは、前述のように、クライアント・ブラウザ２１９によって大容量記憶媒体２４１から読み取り、その後移動再生装

置２１２に転送することができる。図９は、クライアント・コンピュータ２１４を使用した移動再生装置２１２へのデータ転送を含まないシステムの他の実施形態を示す。キオスク９１０は前述の図１で示されるようなコンピュータ・システムから構成される。キオスク９１０は、公的にアクセスできるユニットであり、クライアント・コンピュータ・システム２１４と同様にブラウズ機能、コンテント購入機能、およびダウンロード機能を実行することができる。キオスク９１０は、コンテントの高速ローカル・アクセスおよびダウンロードができるようにそれ自体のライブラリ・サーバを含むので特殊なシステムである。キオスク９１０は、移動装置インタフェース２２１、すなわち、クライアント・ブラウザ２１９の特殊バージョンと、ローカル・ライブラリ・サーバ・プロセス４６０とを含む。キオスク・ライブラリ・サーバ・プロセス４６０は、スクランブルされ圧縮されたデジタル情報ファイル２６２をローカルに記憶する。このような圧縮された情報ファイル２６２は、リモート・オーサリング・システム２８０から発信され、大容量記憶媒体２４１の物理的トランスポートまたは配信網２４０を介して供給することができる。顧客は、クライアント・ブラウザ２１９を操作してデジタル情報ファイルをブラウズし、選択し、購入し、このデジタル情報ファイルが顧客の移動再生装置２１２に供給される。ネットワーク２４０を介してリモート許可サーバ２７０に接続されたライブラリ・サーバ・プロセス４６０によって、認証プロセス、ターゲティング・プロセス、およびダウンロード・プロセスがキオスク内で実行される。関連実施形態で、図７は、ローカル・ライブラリ７１０を含むクライアント・システム２１４を示し、このクライアント・システム２１４は、キオスク９１０と同様な機能を有するキオスクに変換することができる。このシステムでは、クライアント・ブラウザ２１９の特殊バージョンが前述のキオスク実施形態と同じ機能を実現する。

【００５０】

システムの代替実施形態は、共通の通信網を使用してすべてのシステム構成要素を接続する。図１０で、ネットワーク２４０はクライアント・システム２１４および８１４、ネットワーク・インタフェース８１０、ライブラリ・サーバ２６０、許可サーバ２７０、およびオーサリング・システム２８０に直接結合される

。当業者には、システムの機能を変更せずに、ネットワーク２４０をいくつかの独立のネットワークまたは通信リンクにセグメント化することもできることが認識されよう。

【００５１】

前述のように、移動再生装置２１２は、許可されたデジタル情報コンテントのみを再生することが期待される。各移動再生装置２１２に固有のプレーヤーＩＤが埋め込まれる。各移動再生装置２１２は任意選択で１つまたは複数のグループＩＤ値を備えることができる。候補デジタル情報ファイルには１つまたは複数のプレーヤーＩＤおよびグループＩＤが組み込まれる。移動再生装置２１２の組込みソフトウェアは、候補デジタル情報ファイルに埋め込まれたプレーヤーＩＤおよびグループＩＤのリストを検査し、少なくとも１つのプレーヤーＩＤまたはグループＩＤが移動再生装置２１２プレーヤーＩＤまたはグループＩＤと一致する場合、移動再生装置２１２はデジタル情報ファイルを再生する。一致が見つからない場合、移動再生装置２１２はデジタル情報ファイルを再生しない。

【００５２】

移動再生装置２１２へのプレーヤーＩＤの割当ては好ましくは、移動再生装置２１２の製造時に行われる。移動再生装置２１２へのグループＩＤの割当ては、様々な理由で様々な時間に行うことができる。通常、デジタル情報ライブラリからデジタル情報ファイルにアクセスするユーザには、ユーザのアカウントに関連する単一のグループＩＤが割り当てられ、このグループＩＤはユーザの移動再生装置に埋め込まれる。グループＩＤは、ある会社によって維持されている装置に対応する再生装置群、あるいは単一のアカウント保持者の再生装置群、あるいは特殊利益団体またはクラブの会員によって所有されているプレーヤーに埋め込むことができる。

【００５３】

実際には、ユーザがあるデジタル情報ファイルへのアクセスを購入したときと、このデジタル情報ファイルの特殊バージョンをユーザが利用できるようになったときに、ユーザのアカウント特有のグループＩＤがこのデジタル情報ファイルに埋め込まれる。

【００５４】

埋め込まれたプレーヤーＩＤおよびグループＩＤを有する特定のデジタル情報ファイルをターゲティングの趣旨を覆すように変更できないように、図１１に示すように、デジタル署名標準（ＤＳＳ）を使用するセキュリティ方式を実現することが好ましい。１１０１で、ターゲティングすべきデジタル情報ファイルのヘッダに適切なプレーヤーＩＤおよびグループＩＤが組み込まれる。１１０３で、プログラム・データのｎ秒ごとに、安全ハッシュ・アルゴリズム（ＳＨＡ）を使用する安全ハッシュが算出される。１１０５で、ターゲティング中のデジタル情報ファイルに関連する関連データを含むデジタル署名メッセージが作成される。このような情報には以下の情報アイテムを含めることができるが、これらに限らない。

－プログラム・ヘッダ・バージョン番号
－ハッシュ・アルゴリズム・バージョン番号
－プログラム通し番号
－ハッシュ・ブロック・サイズ
－プレーヤーＩＤカウント
－グループＩＤカウント
－グループＩＤリスト
－ハッシュ・テーブル・カウント
－ハッシュ値

【００５５】

本発明との適合性を失わずに、上記のリストにエントリを追加するか、あるいは上記のリストからエントリを削除できることが認識されよう。１１０７で、デジタル署名認証（ＤＳＡ）に関するメッセージが与えられ、１１０９で、結果として得られるデジタル署名がデジタル情報ファイルに埋め込まれる。

【００５６】

ＤＳＡを使用する好ましいプレーヤー・セキュリティ方式を図１２に示す。１２０１で、プログラム・ファイル・ヘッダ、ヘッダ署名、メッセージ、およびプログラム・データの一部がプレーヤーに転送される。プレーヤーは、情報を受信

した後、１２０３でＤＳＡを実行し、送信側、通常はライブラリ・サーバによって作成された署名を認証する。首尾よく認証された場合、プレーヤーは１２０５で、プレーヤーのプレーヤーＩＤおよびグループＩＤを、メッセージに埋め込まれたリストと比較する。少なくとも１つのプレーヤーＩＤまたはグループＩＤが一致する場合、プレーヤーは１２０７で、ライブラリ・サーバからプレーヤーに転送されるプログラム・データのｎ秒部分ごとに安全ハッシュを算出する。算出される各ハッシュがメッセージに存在する場合、プレーヤーは１２０９で、プログラム・データを再生する。本発明との適合性を失わずにＤＳＡ以外の他のプレーヤー・セキュリティ方式を使用できることが認識されよう。たとえば、プログラム・データが確実に、許可された供給源から発信された有効なデータになるように、プライベートを暗号化アルゴリズムと共に使用することができる。

【００５７】

したがって、認証プロトコルおよび暗号化プロトコルを使用したコンピュータ・ネットワーク・ベースのデジタル情報ライブラリ・システムを実現し、デジタル情報ライブラリ・プログラム、ソフトウェア、および構成データをクライアント・コンピュータ・システムおよびクライアント・コンピュータ・システムに着脱可能に接続できる移動デジタル情報再生装置に安全に転送する方法および装置を開示した。特定の例およびサブシステムに関して本発明を説明したが、当業者には、本発明がこれらの特定の例またはサブシステムに限らず、他の実施形態にも拡張されることが明らかになろう。本発明は、特許請求の範囲に指定されるすべてのこれらの他の実施形態を含む。

【図面の簡単な説明】

【図１】

本発明に適合する典型的なコンピュータ・プラットフォームを示す図である。

【図２】

本発明に適合するコンピュータ・ネットワーク・ベースのデジタル情報ライブラリ・システムのハイレベル・ブロック図である。

【図３】

本発明に適合するオーサリング・システムのハイレベル・ブロック図である。

【図４】

複数のライブラリ・サーバを有する代替実施形態を示す図である。

【図５】

複数のライブラリ・サーバ・プロセスを有する代替実施形態を示す図である。

【図６】

単一のオーサリング／許可サーバを有する代替実施形態を示す図である。

【図７】

クライアント・コンピュータ・システムがローカル・ライブラリを有する代替実施形態を示す図である。

【図８】

移動再生装置がクライアント・コンピュータ・システムの代わりに直接ネットワーク・インタフェースを有する代替実施形態を示す図である。

【図９】

選択されたプログラミングを保持し配信するためにキオスクが使用される代替実施形態を示す図である。

【図１０】

すべてのシステム構成要素が共通のネットワークを介して接続される代替実施形態を示す図である。

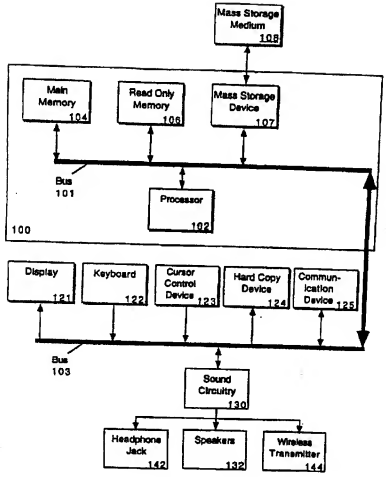
【図１１】

本発明に適合するデジタル署名標準（ＤＳＳ）を使用するセキュリティ方式のフローチャートである。

【図１２】

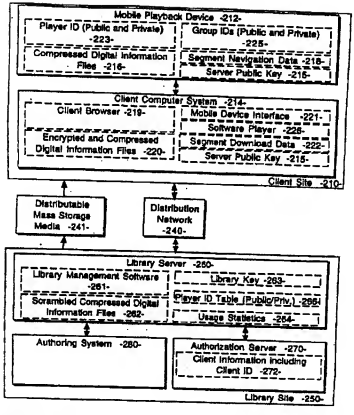
本発明に適合するデジタル署名認証（ＤＳＡ）を使用するプレーヤー・セキュリティ方式のフローチャートである。

【図１】



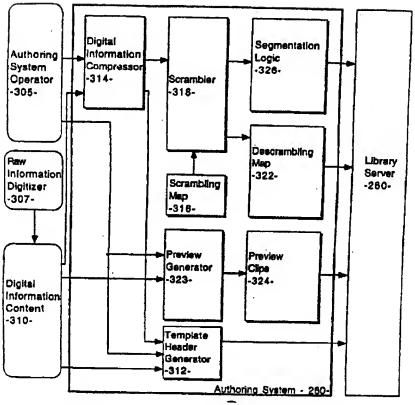
１０１　バス、　１０２　プロセッサ、　１０３　バス、
１０４　メイン・メモリ、　１０６　読取り専用メモリ、１０７　大容量記憶装置、
１０８　大容量記憶媒体、　１２１　ディスプレイ、　１２２　キーボード、
１２３　カーソル制御装置、　１２４　ハード・コピー装置、１２５　通信装置
１３０　音声回路、　１３２　スピーカ、
１４２　ヘッドフォン・ジャック、　１４４　無線送信機

【図２】



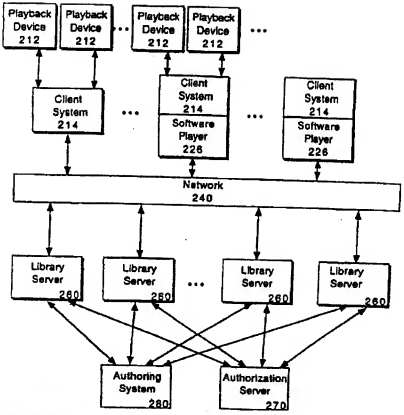
210 クライアント・サイト、
211 移動再生装置、
212 移動プレーヤー、
213 サーバ公開鍵、
214 クライアント・コンピュータ・システム、
215 サーバ公開鍵、
216 圧縮されたデジタル情報ファイル、
217 セグメント・ナビゲーション・データ
218 セグメント・ナビゲーション・データ
219 ブラウザ、
220 暗号化され圧縮されたデジタル情報ファイル
221 移動装置インターフェース、
222 セグメント・ダウンロード・データ
223 プレーヤ・ＩＤ（パブリックおよびプライベート）
225 グループＩＤ（パブリックおよびプライベート）
226 ライブラリ・サイト、
240 配信網、
250 ライブラリ・サイト、
260 ライブラリ管理ソフトウェア
261 ライブラリ管理ソフトウェア
262 圧縮されたデジタル情報ファイル
263 ライブラリ鍵、
264 ライブラリ使用状況統計、
265 プレーヤＩＤテーブル（パブリックおよびプライベート）
270 許可サーバ、
272 クライアントＩＤを含むクライアント情報
280 オーサリング・システム

【図３】



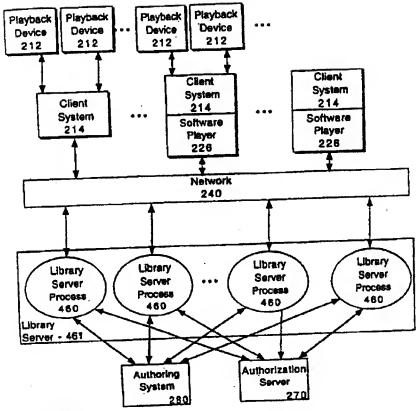
２６０　ライブラリ・サーバ、　　２８０　オーサリング・システム
３０５　オーサリング・システム・オペレータ
３０７　生情報デジタイザ、　　３１０　デジタル情報コンテント
３１２　テンプレート・ヘッダ生成装置
３１４　デジタル情報コンプレッサ
３１６　スクランブル・マップ、　　３１８　スクランブラ
３２２　スクランブル解除マップ、　３２３　プレリビュー・ジェネレータ
３２４　プレビュー・クリップ、　　３２６　セグメント化論理

【図４】



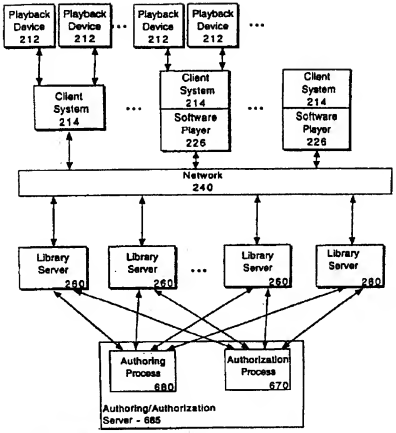
２１２　再生装置、
２２６　ソフトウェア・プレーヤー、
２６０　ライブラリ・サーバ、
２８０　オーサリング・システム
２１４　クライアント・システム
２４０　ネットワーク
２７０　許可サーバ

【図５】



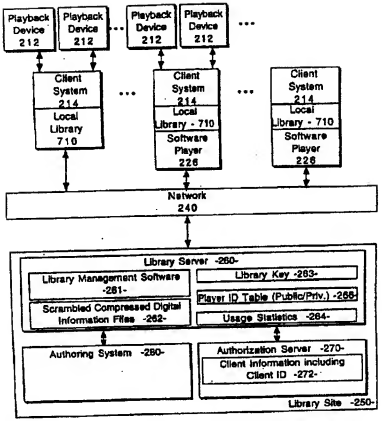
２１２　再生装置、
２２６　ソフトウェア・プレーヤー、
２７０　許可サーバ、
４６０　ライブラリ・サーバ・プロセス
４６１　ライブラリ・サーバ
２１４　クライアント・システム
２４０　ネットワーク
２８０　オーサリング・システム

【図６】



２１２　再生装置、　２１４　クライアント・システム
２２６　ソフトウェア・プレーヤー、　２４０　ネットワーク
２６０　ライブラリ・サーバ、　６７０　許可プロセス
６８０　オーサリング・プロセス、　６８５　オーサリング／許可サーバ

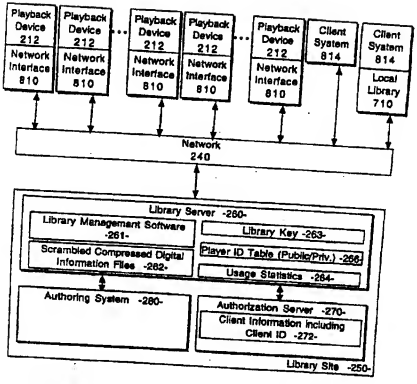
【図７】



２１２　再生装置、
２２５　ソフトウェア・プレーヤー、
２５０　ライブラリ・サイト、
２６１　ライブラリ管理ソフトウェア、
２６３　ライブラリ鍵、
２６６　プレーヤーＩＤテーブル（パブリック／プライベート）
２７０　許可サーバ、　２７２　クライアントＩＤを含むクライアント情報
２８０　オーサリング・システム、

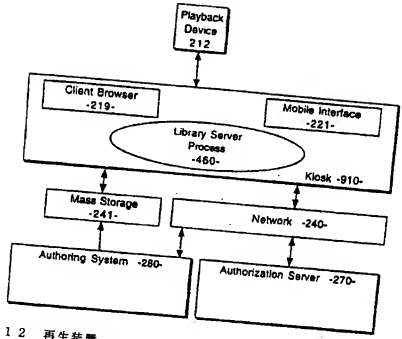
２１４　クライアント・システム
２４０　ネットワーク
２６０　ライブラリ・サーバ
２６２　スクランブルされ圧縮されたデジタル情報ファイル
２６４　使用状況統計
７１０　ローカル・ライブラリ

【図８】



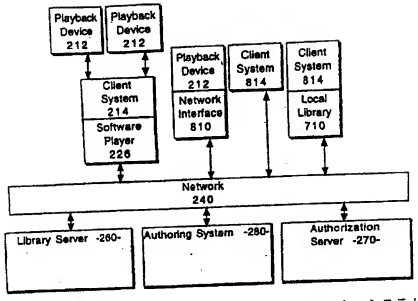
２１２　再生装置、　２４０　ネットワーク、　２５０　ライブラリ・サイト
２６０　ライブラリ・サーバ、　２６１　ライブラリ管理ソフトウェア
２６２　スクランブルされ圧縮されたデジタル情報ファイル
２６３　ライブラリ鍵、　２６４　使用状況統計
２６６　プレーヤーＩＤテーブル（パブリック／プライベート）
２７０　許可サーバ、　２７２　クライアントＩＤを含むクライアント情報
２８０　オーサリング・システム、　７１０　ローカル・ライブラリ
８１０　ネットワーク・インタフェース、　８１４　クライアント・システム

【図９】



２１２　再生装置、
２２１　移動インタフェース、
２４１　大容量記憶域、
２８０　オーサリング・システム
４６０　ライブラリ・サーバ・プロセス
９１０　キオスク
２１９　クライアント・ブラウザ
２４０　ネットワーク
２７０　許可サーバ

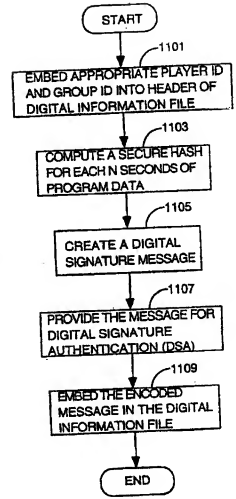
【図１０】



２１２　再生装置、
２２６　ソフトウェア・プレーヤー、
２６０　ライブラリ・サーバ、
２８０　オーサリング・システム、
８１０　ネットワーク・インタフェース
８１４　クライアント・システム
２１４　クライアント・システム
２４０　ネットワーク
２７０　許可サーバ
７１０　ローカル・ライブラリ

【図１１】

１１０１　デジタル情報ファイルのヘッダに適切なプレーヤーＩＤおよびグループＩＤを埋め込む。
１１０３　プログラム・データのｎ秒ごとに安全ハッシュを算出する。
１１０５　デジタル署名メッセージを作成する。
１１０７　デジタル署名認証（ＤＳＡ）に関するメッセージを与える。
１１０９　コード化されたメッセージをデジタル情報ファイルに埋め込む。



【図１２】

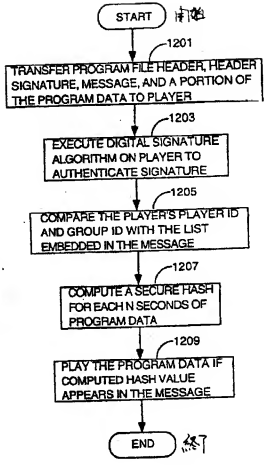
１２０１　プログラム・ファイル・ヘッダ、ヘッダ署名、メッセージ、およびプログラム・データの一部をプレーヤーに転送する。

１２０３　プレーヤー上でデジタル署名アルゴリズムを実行し署名を認証する。

１２０５　プレーヤーのプレーヤーＩＤおよびグループＩＤを、メッセージに埋め込まれたリスト比較する。

１２０７　プログラム・データのｎ秒ごとに安全ハッシュを算出する。

１２０９　算出されたハッシュ値がメッセージに存在する場合にプログラム・データを再生する。



【手続補正書】

【提出日】平成１２年５月１０日（２０００．５．１０）

【手続補正１】

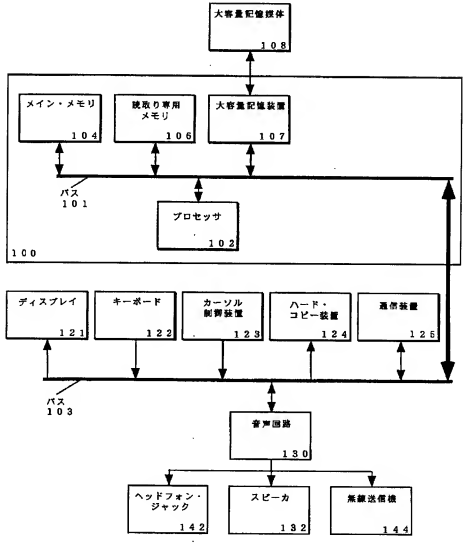
【補正対象書類名】図面

【補正対象項目名】全図

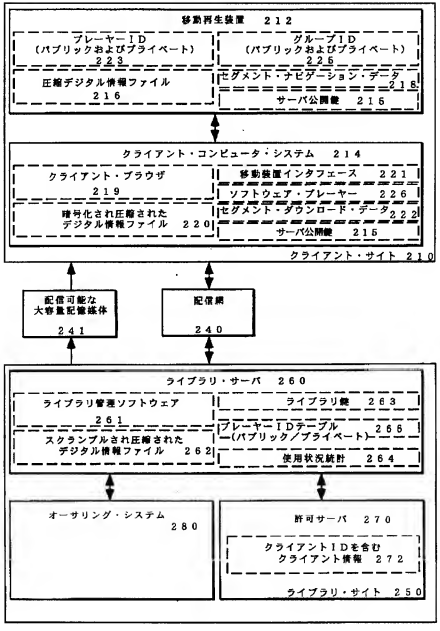
【補正方法】変更

【補正内容】

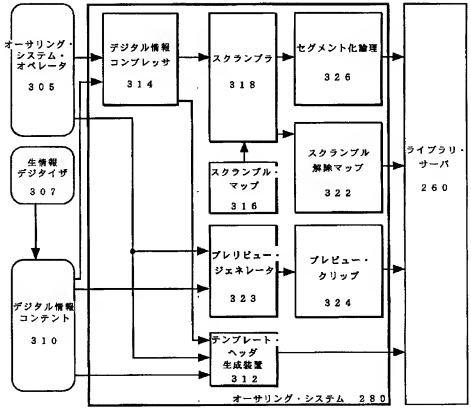
【図１】



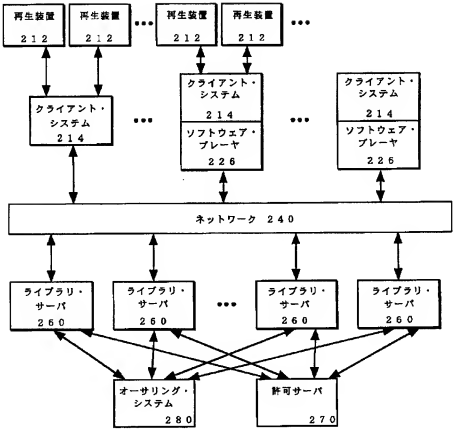
【図２】


移動再生装置 ２１２
プレーヤーＩＤ（パブリックおよびプライベート）２２３
グループＩＤ（パブリックおよびプライベート）２２６
圧縮デジタル情報ファイル ２１６
セグメント・ナビゲーション・データ ２１８
サーバ公開鍵 ２１５
クライアント・コンピュータ・システム ２１４
クライアント・ブラウザ ２１９
移動装置インタフェース ２２１
ソフトウェア・プレーヤー ２２６
暗号化され圧縮されたデジタル情報ファイル ２２０
セグメント・ダウンロード・データ ２２２
サーバ公開鍵 ２１５
クライアント・サイト ２１０
配信可能な大容量記憶媒体 ２４１
配信網 ２４０
ライブラリ・サーバ ２６０
ライブラリ管理ソフトウェア ２６１
ライブラリ鍵 ２６３
プレーヤーＩＤテーブル（パブリック／プライベート）２６５
スクランブルされ圧縮されたデジタル情報ファイル ２６２
使用状況統計 ２６４
オーサリング・システム ２８０
許可サーバ ２７０
クライアントＩＤを含むクライアント情報 ２７２
ライブラリ・サイト ２５０

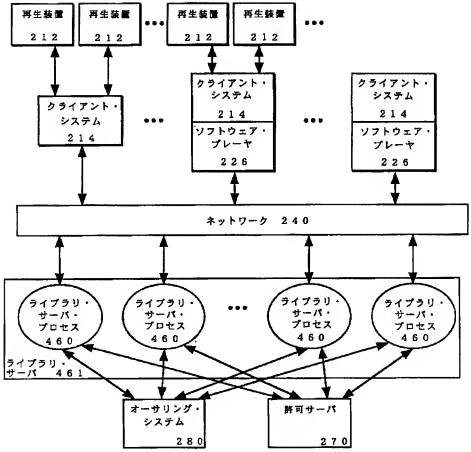
【図３】


オーサリング・システム・オペレータ
３０５
生情報デジタイザ
３０７
デジタル情報コンテント
３１０
デジタル情報コンプレッサ
３１４
スクランブラ
３１８
セグメント化論理
３２６
スクランブル・マップ
３１６
スクランブル解除マップ
３２２
プレリビュー・ジェネレータ
３２３
プレビュー・クリップ
３２４
テンプレート・ヘッダ生成装置
３１２
ライブラリ・サーバ
２６０
オーサリング・システム　２８０

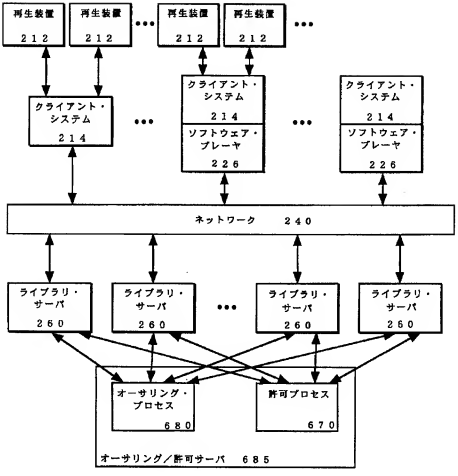
【図４】


再生装置
２１２
再生装置
２１２
再生装置
２１２
再生装置
２１２
クライアント・システム
２１４
クライアント・システム
２１４
ソフトウェア・プレーヤ
２２６
クライアント・システム
２１４
ソフトウェア・プレーヤ
２２６
ネットワーク ２４０
ライブラリ・サーバ
２６０
ライブラリ・サーバ
２６０
ライブラリ・サーバ
２６０
ライブラリ・サーバ
２６０
オーサリング・システム
２８０
許可サーバ
２７０

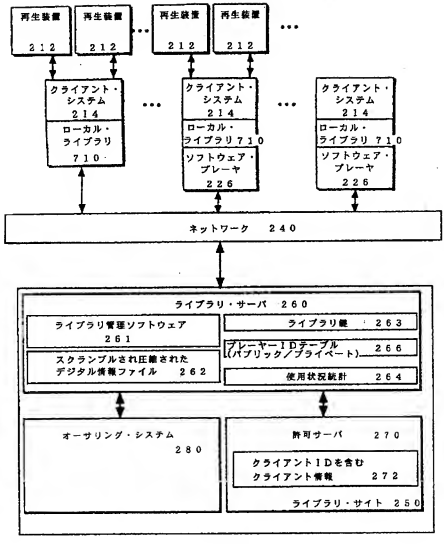
【図５】


再生装置
２１２
再生装置
２１２
再生装置
２１２
再生装置
２１２
クライアント・システム
２１４
クライアント・システム
２１４
ソフトウェア・プレーヤ
２２６
クライアント・システム
２１４
ソフトウェア・プレーヤ
２２６
ネットワーク ２４０
ライブラリ・サーバ・プロセス
４６０
ライブラリ・サーバ・プロセス
４６０
ライブラリ・サーバ・プロセス
４６０
ライブラリ・サーバ・プロセス
４６０
ライブラリ・サーバ ４６１
オーサリング・システム
２８０
許可サーバ
２７０

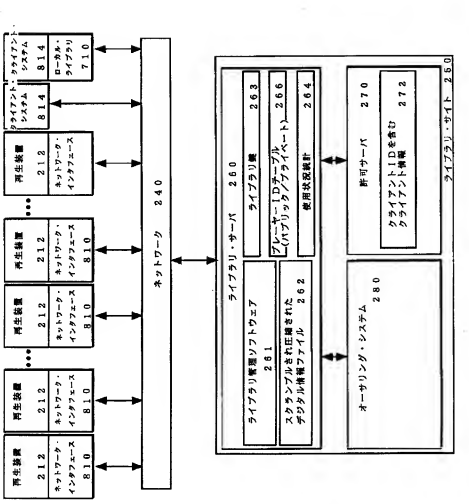
【図６】


再生装置
２１２
再生装置
２１２
再生装置
２１２
再生装置
２１２
クライアント・システム
２１４
クライアント・システム
２１４
ソフトウェア・プレーヤ
２２６
クライアント・システム
２１４
ソフトウェア・プレーヤ
２２６
ネットワーク　２４０
ライブラリ・サーバ
２６０
ライブラリ・サーバ
２６０
ライブラリ・サーバ
２６０
ライブラリ・サーバ
２６０
オーサリング・プロセス
６８０
許可プロセス
６７０
オーサリング／許可サーバ　６８５

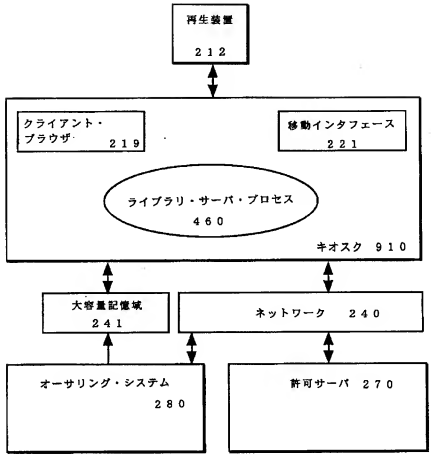
【図７】


再生装置 212
再生装置 212
再生装置 212
再生装置 212
クライアント・システム 214
ローカル・ライブラリ 710
クライアント・システム 214
ローカル・ライブラリ 710
ソフトウェア・プレーヤ 226
クライアント・システム 214
ローカル・ライブラリ 710
ソフトウェア・プレーヤ 226
ネットワーク 240
ライブラリ・サーバ 260
ライブラリ管理ソフトウェア 261
スクランブルされ圧縮されたデジタル情報ファイル 262
ライブラリ鍵 263
プレーヤーIDテーブル (パブリック/プライベート) 266
使用状況統計 264
オーサリング・システム 280
許可サーバ 270
クライアントIDを含むクライアント情報 272
ライブラリ・サイト 250

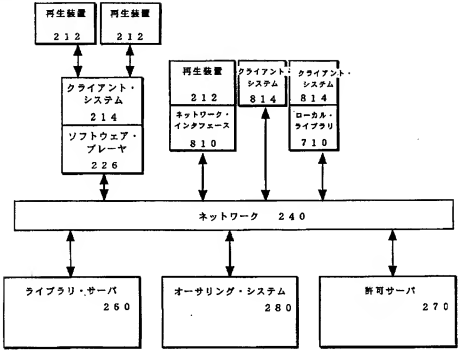
【図８】


再生装置 212
ネットワーク・インタフェース 810
クライアント・システム 814
ローカル・ライブラリ 710
ネットワーク 240
ライブラリ・サーバ 260
ライブラリ管理ソフトウェア 261
ライブラリ簿 263
プレーヤーIDウォーターマーク（パブリック及びプライベート） 265
使用状況統計 264
スタンプ化され圧縮されたデジタル情報ファイル 262
オーサリング・システム 280
許可サーバ 270
クライアントIDを含むクライアント情報 272
ライブラリ・サイト 250

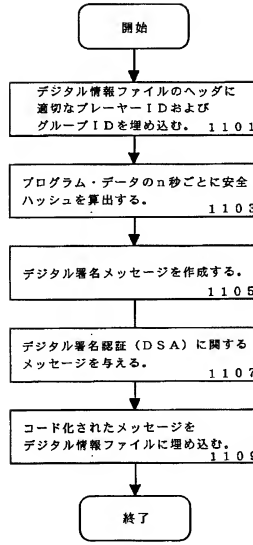
【図９】


再生装置
２１２
クライアント・
ブラウザ
２１９
移動インタフェース
２２１
ライブラリ・サーバ・プロセス
４６０
キオスク ９１０
大容量記憶域
２４１
ネットワーク ２４０
オーサリング・システム
２８０
許可サーバ ２７０

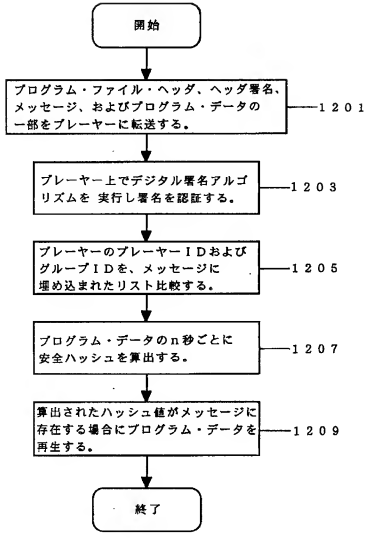
【図１０】


再生装置
２１２
再生装置
２１２
クライアント・システム
２１４
ソフトウェア・プレーヤ
２２６
再生装置
２１２
ネットワーク・インタフェース
８１０
クライアント・システム
８１４
クライアント・システム
８１４
ローカル・ライブラリ
７１０
ネットワーク　２４０
ライブラリ・サーバ
２５０
オーサリング・システム
２８０
許可サーバ
２７０

【図１１】


開始
デジタル情報ファイルのヘッダに
適切なプレーヤーＩＤおよび
グループＩＤを埋め込む。 １１０１
プログラム・データのｎ秒ごとに安全
ハッシュを算出する。
１１０３
デジタル署名メッセージを作成する。
１１０５
デジタル署名認証（ＤＳＡ）に関する
メッセージを与える。
１１０７
コード化されたメッセージを
デジタル情報ファイルに埋め込む。
１１０９
終了

【図１２】


開始
プログラム・ファイル・ヘッダ、ヘッダ署名、メッセージ、およびプログラム・データの一部をプレーヤーに転送する。
１２０１
プレーヤー上でデジタル署名アルゴリズムを 実行し署名を認証する。
１２０３
プレーヤーのプレーヤーＩＤおよびグループＩＤを、メッセージに埋め込まれたリスト比較する。
１２０５
プログラム・データのｎ秒ごとに安全ハッシュを算出する。
１２０７
算出されたハッシュ値がメッセージに存在する場合にプログラム・データを再生する。
１２０９
終了

【国際調査報告】

INTERNATIONAL SEARCH REPORT

International application No. PCT/US98/20659

A. CLASSIFICATION OF SUBJECT MATTER
IPC(6) :G06F 11/00
US CL :395/186
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
U.S. : 395/186, 188.01; 380/23, 25

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Microsoft Press Computer Dictionary 2nd Edition

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
APS

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 5,483,658 A (GRUBE et al) 09 January 1996; Figure 1 and 2; Abstract; col. 3, lines 31-67; col. 4, lines 1-16 and 30-48; col. 5, lines 46-67; col. 6, lines 1-33.	1-2, 7-8, 13-14, 19-20, 25-26, 31-32 and 37
Y	US 5,483,658 A (GRUBE et al) 09 January 1996; Figures 1 and 2; Abstract; col. 3, lines 31-67; col. 4, lines 1-16 and 30-48; col. 5, lines 46-67; col. 6, lines 1-33.	3, 9, 15, 21, 27 and 33
Y	MICROSOFT PRESS, Computer Dictionary 2nd edition, 1994, pp. 194-195.	3, 9, 15, 21, 27 and 33
A	US 5,511,122 A (ATKINSON) 23 April 1996; see entire document.	1-37

[X] Further documents are listed in the continuation of Box C [ ] See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier document published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
29 DECEMBER 1998	24 FEB 1999
Name and mailing address of the ISA/US Commissioner of Patents and Trademarks Box PCT Washington, D.C. 20231 Facsimile No. (703) 305-3230	Authorized officer ROBERT BEAUSOLIEL Telephone No. (703) 305-9713

Form PCT/ISA/210 (second sheet)(July 1992)*

INTERNATIONAL SEARCH REPORT

International application No. PCT/US98/20659

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A,P	US 5,781,723 A (YEE et al.) 14 July 1998; see entire document.	1-37
A	US 5,555,098 A (PARULSKI) 10 September 1996; see entire document.	1-37
A	US 5,132,992 A (YURT et al) 21 July 1992; see entire document.	1-37

Form PCT/ISA/210 (continuation of second sheet)(July 1992)*

フロントページの続き

(81)指定国 EP(AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OA(BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG), AP(GH, GM, KE, LS, MW, SD, SZ, UG, ZW), EA(AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), AL, AM, AT, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, UZ, VN, YU, ZW

(72)発明者 ジャン，ベンジャミン・チェーミン
アメリカ合衆国・94303・カリフォルニア州・パロ アルト・タンランド ドライブ・1081－ビイ

(72)発明者 ベイ，サミュエル・ホンーイェン
アメリカ合衆国・92009・カリフォルニア州・カールスバッド・ピラグア ストリート・3306

(72)発明者 コチャー，ポール
アメリカ合衆国・94117・カリフォルニア州・サン フランシスコ・フィルモア ストリート・143

Fターム(参考) 5B017 AA06 BA09 BB09 CA16
5D044 AB01 AB05 BC01 BC02 CC04 DE49 GK12 HL11
5J104 AA07 AA09 AA16 EA04 EA26 KA02 KA06 KA09 LA03 LA06 MA02 NA12 PA11